



# FortiOS - New Features Guide

Version 6.4.0

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



June 08, 2023

FortiOS 6.4.0 New Features Guide

01-640-582010-20230608



# TABLE OF CONTENTS

<b>Change Log</b>	<b>9</b>
<b>GUI</b>	<b>12</b>
Getting started	12
Firmware upgrade notifications	12
Transfer a device to another FortiCloud account 6.4.1	13
FortiCare registration disclaimer 6.4.1	15
Dashboards and widgets	16
Consolidate Monitor and FortiView pages	16
IP address tooltips	22
View session information for a compromised host 6.4.1	24
Consolidated dashboard usability improvements 6.4.1	25
Add detachable CLI console tabs 6.4.2	31
Implement a user device store to centralize device data 6.4.3	32
<b>Security Fabric</b>	<b>34</b>
Fabric settings	34
Integrate FortiAnalyzer management into the Security Fabric using SAML SSO	34
Simplify FortiClient EMS setup	37
Simplify the synchronization of EMS tags and configurations	40
Allow FortiNAC to join the Security Fabric	42
Redesign Fortinet Fabric Connectors and Fabric setup pages	44
Display endpoints in Topology using donut chart	47
Using the root FortiGate with disk to store historic user and device information	49
Synchronizing objects across the Security Fabric	49
Streamlined Fortinet Security Fabric setup between FortiGates 6.4.2	53
Use an FQDN in FortiSandbox fabric connectors 6.4.2	55
FortiMail Security Fabric integration 6.4.2	56
Allow EMS Cloud configuration only when the entitlement is verified 6.4.3	60
Improvements to synchronizing objects across the Security Fabric 6.4.4	62
Detect FortiManager Cloud account level subscription 6.4.4	69
SDN connectors	71
SDN connector for Cisco ACI northbound API integration	71
Support multiple SDN connector instances for Cisco ACI and Nuage	74
Multifunction tooltip for Fabric connectors	81
Exchange Server connector with Kerberos KDC auto-discovery	82
Support IBM Cloud SDN connector 6.4.1	83
Support ServiceTag and Region for Azure SDN connector address objects 6.4.2	87
Multiple IP addresses on Cisco ACI connectors 6.4.4	89
Multiple clusters on Cisco ACI connectors 6.4.9	93
Update OpenStack SDN connector to support the latest OpenStack releases 6.4.9	96
Automation stitches	99
Automation stitches	100
Slack notification action	109
NSX-T quarantine action 6.4.1	113
FortiNAC quarantine action for automation 6.4.2	116
Security ratings	120

Redesign Security Rating scorecards .....	121
Tests for FortiSwitch added to Security Rating 6.4.2 .....	122
Security rating report in multi VDOM mode 6.4.3 .....	126
<b>Network .....</b>	<b>129</b>
SD-WAN .....	129
SD-WAN event log subtype .....	129
SD-WAN logging improvement to identify matched application .....	133
SD-WAN configuration portability .....	134
SD-WAN log format improvements .....	136
SD-WAN monitor on ADVPN shortcuts .....	142
SD-WAN GUI and monitoring enhancements .....	143
Enhance ADVPN to support UDP hole punching for spokes behind NAT .....	147
SD-WAN health check packet enhancement .....	151
Weighted round robin for IPsec aggregate tunnels .....	151
Default_DNS performance SLA profile .....	153
Interface speedtest .....	154
Support SD-WAN integration with OCVPN .....	156
Allow FortiClient to join OCVPN .....	164
Support SD-WAN interface as a security zone 6.4.1 .....	168
ADVPN hub and spoke VPN Wizard improvements 6.4.2 .....	172
Allow MAC addresses to be used in SD-WAN rules and policy routes 6.4.2 .....	176
Up to 1024 spokes in OCVPN 6.4.2 .....	177
SD-WAN enhancements 6.4.2 .....	178
Define SD-WAN duplication rules to duplicate packets on other members of the SD-WAN zone 6.4.2 .....	182
Allow packet duplication on SD-WAN based on SD-WAN rules 6.4.3 .....	184
BGP additional path limit increased to 255 6.4.3 .....	186
SD-WAN IPv6 route tag 6.4.4 .....	186
REST API to monitor SD-WAN SLAs for ADVPN shortcuts 6.4.5 .....	188
General .....	191
Route leaking between VRFs .....	191
IBGP and EBGP support in VRF .....	193
Set minimum RIP update timer to one second .....	196
DHCP client options .....	196
Assign a subnet to FortiGate with the FortiIPAM service 6.4.1 .....	197
VRF GUI support 6.4.2 .....	204
Determine if recursive distance is evaluated in BGP's next hops under ECMP 6.4.2 .....	206
PRP on SoC4 models 6.4.3 .....	207
FN-TRAN-DSL module on FG-80F and FGR-60F-3G4G 6.4.9 .....	208
Reset the VLAN DEI bit when passing through a FortiGate in NAT mode 6.4.9 .....	210
FS-TRANS-FX module on FGR-60F and FGR-60F-3G4G 6.4.9 .....	211
Inspect double-tagged traffic on virtual wire pairs 6.4.9 .....	212
Support 802.1X on virtual switch for certain NP6 platforms 6.4.10 .....	213
IPv6 .....	213
IPv6 geography-based address support .....	213
Support for IPv6 in central SNAT table .....	215
FQDN support for remote gateways .....	217
MAP-E support 6.4.1 .....	219
IPv6 MAC addresses and usage in firewall policies 6.4.2 .....	223

Web proxy .....	225
Authentication support for upstream proxy in transparent proxy mode .....	225
Support TLS 1.3 for proxy forward servers in certificate inspection mode 6.4.1 .....	227
<b>System .....</b>	<b>229</b>
General .....	229
Admin profile option for diagnostic access .....	229
FortinetOne renamed FortiCloud .....	230
No session timeout .....	231
Confirmation prompt when creating new VDOMs .....	232
FortiOS image signing and verification .....	233
Consistent style for replacement messages 6.4.2 .....	233
Introduce maturity firmware levels 6.4.10 .....	235
Enhance BIOS-level signature and file integrity checking 6.4.13 .....	236
High availability .....	236
Force HA failover for testing and demonstrations .....	236
Support UTM inspection on asymmetric traffic in FGSP .....	239
Support UTM inspection on asymmetric traffic on L3 .....	241
Add encryption for L3 on asymmetric traffic in FGSP .....	243
Override FortiAnalyzer and syslog server settings .....	243
Source interface setting for NetFlow data .....	247
Applying the session synchronization filter only between FGSP peers in an FGCP over FGSP topology 6.4.10 .....	249
SNMP .....	249
SNMP bridge MIB module support .....	249
Support SHA-2 for SNMPv3 .....	251
SNMP traps and query for monitoring DHCP pool .....	252
SNMP polling extensions to support new OIDs 6.4.2 .....	253
SNMP OIDs for port block allocations IP pool statistics 6.4.12 .....	255
FortiGuard .....	255
Use anycast to communicate with FortiGuard servers .....	256
IoT detection service .....	258
Display cloud service communications statistics .....	260
Support third party CA signed certificates with OCSP stapling 6.4.2 .....	261
FDS-only ISDB package in firmware images 6.4.10 .....	261
<b>Policy and Objects .....</b>	<b>262</b>
Policies .....	262
Support SSL mirroring in proxy mode .....	262
Consolidated IPv4 and IPv6 policy configuration .....	265
UUID field added to all policy types .....	267
SNAT support for policies with virtual wire pairs .....	269
Interface-based traffic shaping with NP acceleration .....	271
Ingress traffic shaping profile 6.4.7 .....	273
Objects .....	279
Array structure for address objects .....	279
Allow creation of ISDB objects with regional information .....	281
IP definitions database merged into the internet service database .....	283
Extend ISDB to include well-known MAC address list .....	285
GeoIP matching by registered and physical location .....	286

Group address objects synchronized from FortiManager .....	288
Increase in maximum number of VIP real servers .....	290
GUI support for real server configurations using address objects 6.4.2 .....	290
<b>Security profiles .....</b>	<b>292</b>
Antivirus .....	292
Security Profiles enhancements .....	292
Antivirus uses the extended database by default .....	298
Scan compressed messages over CIFS protocol in proxy mode 6.4.2 .....	299
Application control .....	300
SSL-based application detection over decrypted traffic in a sandwich topology .....	301
Matching multiple parameters on application control signatures .....	301
Allow exclusion of signatures in application control profile 6.4.3 .....	304
Web filter .....	306
Credential phishing prevention .....	306
Explicitly enable custom categories for web filter profiles, SSL/SSH inspection profiles, and proxy addresses 6.4.2 .....	308
Configure web filter profiles in NGFW policy mode 6.4.2 .....	312
Remove the option to rate images by URL in Web filter profiles 6.4.3 .....	315
Rating submission link on web filter block and warning pages 6.4.5 .....	315
IPS .....	316
Detecting IEC 61850 MMS protocol in IPS .....	316
IPS signature filter options 6.4.2 .....	318
Others .....	320
Redirect to WAD after handshake completion .....	320
ICAP response filtering .....	321
Separate file filter into a standalone profile 6.4.1 .....	323
Handling SSL offloaded traffic from an external decryption device in flow mode 6.4.4 .....	325
<b>VPN .....</b>	<b>328</b>
IPsec and SSL VPN .....	328
Dynamic address support for SSL VPN policies .....	328
NAS-IP support per SSL VPN realm .....	337
Support defining gateway IP addresses in IPsec with mode-config and DHCP .....	339
Provision SSL VPN users in FortiClient Mobile with an email or SMS message 6.4.2 .....	341
Configure DSCP for IPsec tunnels 6.4.3 .....	341
<b>User and authentication .....</b>	<b>344</b>
Authentication .....	344
SAML SP for VPN authentication .....	344
Support for Okta RADIUS attributes filter-Id and class .....	347
Multiple LDAP servers in Kerberos keytabs and agentless NTLM domain controllers 6.4.3 .....	349
Traffic shaping based on dynamic RADIUS VSAs 6.4.6 .....	350
<b>Secure access .....</b>	<b>358</b>
Wireless .....	358
Wireless IPv6 support .....	358
Support for spectrum analysis of FortiAP E models .....	364
Increase in maximum number of managed FortiAPs .....	370
Even distribution of FortiAP reports .....	371

View detailed information for individual WiFi connections .....	375
VLAN probe report .....	383
FortiAP client load balancing per AP .....	387
Layer three ACL configurations for Wireless APs .....	388
Maintain radio SSID WLAN IDs .....	390
Support for FAP431F and FAP433F .....	392
Support logging the signal-to-noise ratio and signal strength per client 6.4.1 .....	396
Simplify BLE profiles to support broadcast of FortiAP UUID 6.4.2 .....	398
Add ARP profile for wireless controller 6.4.2 .....	401
Extend spectrum analysis to support FortiAPs with three radios 6.4.2 .....	403
Antenna Rx chain status check and notification 6.4.2 .....	409
Standardize wireless health metrics 6.4.2 .....	410
FortiAP query to FortiGuard IoT service to determine device details 6.4.2 .....	414
Enhance MPSK functionalities for wireless controller 6.4.2 .....	415
Adaptive radio architecture support 6.4.3 .....	418
Support 802.11v optimized roaming and load balancing 6.4.3 .....	422
Support IGMP Snooping (Wireless) 6.4.3 .....	424
Use FortiGate to register managed FortiAP to FortiCloud 6.4.3 .....	428
Add fields for wireless DHCP logs 6.4.3 .....	431
Dynamic VLAN assignment using RADIUS attribute string 6.4.6 .....	431
Switch controller .....	433
Switch controller - quarantine by redirect .....	434
VLAN interface templates for FortiSwitch devices .....	436
Improved FortiSwitch support .....	440
GUI support for FortiLink groups .....	440
FortiSwitch link status visibility improvements .....	441
SNMP queries to the FortiGate Switch Controller for FortiSwitch and port information 6.4.2 .....	442
Allow FortiSwitch Trunk mode selection on FortiGate 6.4.2 .....	444
Send multiple RADIUS attribute values in a single RADIUS Access-Request 6.4.2 .....	445
ECN configuration for managed FortiSwitch devices 6.4.2 .....	445
Configure PTP Transparent Clock mode for managed FortiSwitch devices 6.4.2 .....	446
Inter-operability with per instance RSTP 802.1w 6.4.2 .....	447
FortiGate HA between remote sites over managed FortiSwitches 6.4.2 .....	447
Register FortiSwitch to FortiCloud from the GUI 6.4.2 .....	452
GUI support for multiple FortiLink interfaces 6.4.2 .....	455
Switch controller option to control the sources used to update the user device list 6.4.2 .....	459
Log sub-category for switch controller 6.4.3 .....	460
Configure LLDP settings on a switch port that is leased to a tenant VDOM 6.4.3 .....	461
Add a RADIUS timeout VLAN to a security policy 6.4.3 .....	462
Add option to enable flow control and pause metering 6.4.3 .....	462
Allow switch controller to set source IP for outbound connections 6.4.3 .....	463
Enable IoT background scanning 6.4.3 .....	464
NAC .....	464
Support NAC policies on switch ports .....	465
Added ability in FortiSwitch to query FortiGuard IoT service for device details .....	468
FortiSwitch voice device detection .....	470
Extend NAC matching condition to include EMS tags 6.4.2 .....	474

FortiExtender .....	475
Support FortiExtender models with two modems 6.4.2 .....	476
Support data plan profiles for FortiExtender 6.4.2 .....	479
<b>Log and report .....</b>	<b>482</b>
Logging .....	482
Log buffer on FortiGates with an SSD disk .....	482
WAD and Proxyd SSL logging improvement .....	485
WAN interface bandwidth log .....	489
Include RSSO information for authenticated destination users in logs 6.4.1 .....	491
Application logging in NGFW policy mode 6.4.2 .....	494
Send traffic logs to FortiAnalyzer Cloud 6.4.4 .....	495
Log updates to dynamic objects 6.4.5 .....	498
<b>Cloud .....</b>	<b>501</b>
Public and private cloud .....	501
Simplify Azure Fabric connector configuration for a FortiGate-VM deployed on Azure .....	501
Support filtering on AWS autoscaling group for dynamic address objects .....	504
Support dynamic address objects in real servers under virtual server load balance .....	505
Support up to 24 interfaces on FortiGate VM .....	506
Enhanced autoscale clusters for FortiGate VM .....	508
Support FortiGate-VM in IBM Cloud platform 6.4.2 .....	509
Obtaining a FortiCare-generated license for Azure on-demand instances 6.4.2 .....	514
Configure FQDN-based VIPs from the GUI 6.4.2 .....	515
Enhance the display of VM autoscale member information 6.4.2 .....	516
Support for new VM bandwidth-limited SKUs 6.4.2 .....	517
FOS support of VM-ELA (FortiFlex) 6.4.2 .....	521
Liveness detection on NSX-T 6.4.3 .....	523
Add FIPS cipher mode for AWS and Azure FortiGate VMs 6.4.3 .....	523
IMDSv2 for FortiGate-VM on AWS 6.4.3 .....	525
Add VDOM support for NSX-T 6.4.3 .....	525
Support OCI compute shapes that use Mellanox network cards 6.4.3 .....	527
Support AWS transit gateway connect attachment and connect peer 6.4.3 .....	530
Support OCI IMDSv2 6.4.4 .....	534
GENEVE support for AWS gateway load balancer 6.4.4 .....	537
Nutanix service chaining 6.4.5 .....	538
Support multiple GCP projects in a single SDN connector 6.4.7 .....	545
Ciphers added to fips-ciphers mode on FortiGate-VM 6.4.7 .....	549
<b>FortiCarrier .....</b>	<b>550</b>
GTP .....	550
IPv6 support for GTP 6.4.2 .....	550
Add fields to correlate between traffic, GTP, and UTM logs 6.4.2 .....	552
Multiple identities from the ULI field in GTP logs 6.4.2 .....	554
NPU support for GTP-U encapsulated in IPv6 6.4.3 .....	554
<b>FortiASIC .....</b>	<b>557</b>
Hardware acceleration .....	557
Use CP9/SoC3 entropy source .....	557
Identify the XAUI link used for a specific traffic stream .....	557

# Change Log

Date	Change Description
2023-06-08	Initial release of FortiOS 6.4.13.
2023-02-23	Initial release of FortiOS 6.4.12.
2023-01-24	Updated <a href="#">Send traffic logs to FortiAnalyzer Cloud</a> 6.4.4 on page 495.
2022-08-30	Added <a href="#">FDS-only ISDB package</a> in firmware images 6.4.10 on page 261.
2022-08-25	Initial release of FortiOS 6.4.10.
2022-06-15	Added <a href="#">Ingress traffic shaping profile</a> 6.4.7 on page 273.
2022-04-28	Added <a href="#">Inspect double-tagged traffic on virtual wire pairs</a> 6.4.9 on page 212.
2022-04-26	Initial release of FortiOS 6.4.9.
2022-04-14	Added <a href="#">Support AWS transit gateway connect attachment and connect peer</a> 6.4.3 on page 530 and <a href="#">GENEVE support for AWS gateway load balancer</a> 6.4.4 on page 537.
2022-03-10	Updated <a href="#">Transfer a device to another FortiCloud account</a> 6.4.1 on page 13.
2022-03-08	Added <a href="#">Allow EMS Cloud configuration only when the entitlement is verified</a> 6.4.3 on page 60.
2022-03-04	Added <a href="#">Nutanix service chaining</a> 6.4.5 on page 538.
2021-11-08	Updated <a href="#">FortiNAC quarantine action for automation</a> 6.4.2 on page 116.
2021-08-26	Initial release of FortiOS 6.4.7.
2021-05-31	Added <a href="#">Dynamic VLAN assignment using RADIUS attribute string</a> 6.4.6 on page 431.
2021-05-26	Added <a href="#">PRP on SoC4 models</a> 6.4.3 on page 207 and <a href="#">Traffic shaping based on dynamic RADIUS VSAs</a> 6.4.6 on page 350.
2021-05-20	Initial release of FortiOS 6.4.6.
2021-05-17	Updated <a href="#">FortiMail Security Fabric integration</a> 6.4.2 on page 56.
2021-03-08	Added <a href="#">REST API to monitor SD-WAN SLAs for ADVPN shortcuts</a> 6.4.5 on page 188.
2021-02-18	Initial release of FortiOS 6.4.5.
2021-01-25	Updated <a href="#">Antivirus uses the extended database by default</a> on page 298.
2021-01-21	Updated <a href="#">Matching multiple parameters on application control signatures</a> on page 301.
2021-01-14	Added <a href="#">Detect FortiManager Cloud account level subscription</a> 6.4.4 on page 69.
2020-12-10	Initial release of FortiOS 6.4.4.
2020-11-27	Added <a href="#">Determine if recursive distance is evaluated in BGP's next hops under ECMP</a> 6.4.2 on page 206.

Date	Change Description
2020-11-12	Added <a href="#">FOS support of VM-ELA (FortiFlex) 6.4.2 on page 521</a> .
2020-11-06	Added <a href="#">Liveness detection on NSX-T 6.4.3 on page 523</a>
2020-11-04	Added <a href="#">FortiMail Security Fabric integration 6.4.2 on page 56</a> .
2020-10-30	Added <a href="#">Configure DSCP for IPsec tunnels 6.4.3 on page 341</a> and <a href="#">Remove the option to rate images by URL in Web filter profiles 6.4.3 on page 315</a> .
2020-10-29	Added <a href="#">Allow packet duplication on SD-WAN based on SD-WAN rules 6.4.3 on page 184</a> .
2020-10-22	Initial release of FortiOS 6.4.3.
2020-10-02	Guide reorganized.
2020-09-23	Updated <a href="#">SNAT support for policies with virtual wire pairs on page 269</a> .
2020-09-22	Added <a href="#">Switch controller option to control the sources used to update the user device list 6.4.2 on page 459</a> .
2020-08-20	Added <a href="#">Use an FQDN in FortiSandbox fabric connectors 6.4.2 on page 55</a> .
2020-08-14	Updated <a href="#">Obtaining a FortiCare-generated license for Azure on-demand instances 6.4.2 on page 514</a> .
2020-08-07	Added <a href="#">GUI support for multiple FortiLink interfaces 6.4.2 on page 455</a> and <a href="#">Obtaining a FortiCare-generated license for Azure on-demand instances 6.4.2 on page 514</a> .
2020-08-06	Added <a href="#">Tests for FortiSwitch added to Security Rating 6.4.2 on page 122</a> and <a href="#">Provision SSL VPN users in FortiClient Mobile with an email or SMS message 6.4.2 on page 341</a> .
2020-07-30	Initial release of FortiOS 6.4.2.
2020-06-12	Added <a href="#">MAP-E support 6.4.1 on page 219</a> .
2020-06-08	Added <a href="#">Consolidated dashboard usability improvements 6.4.1 on page 25</a> .
2020-06-04	Initial release of FortiOS 6.4.1.
2020-05-13	Updated <a href="#">Credential phishing prevention on page 306</a> .
2020-05-14	Added <a href="#">Array structure for address objects on page 279</a> .
2020-04-06	Added <a href="#">Support filtering on AWS autoscaling group for dynamic address objects on page 504</a> and <a href="#">Support dynamic address objects in real servers under virtual server load balance on page 505</a> .
2020-04-07	Added <a href="#">Allow FortiClient to join OCVPN on page 164</a> , <a href="#">Redesign Fortinet Fabric Connectors and Fabric setup pages on page 44</a> , <a href="#">Display endpoints in Topology using donut chart on page 47</a> , and <a href="#">Consolidate Monitor and FortiView pages on page 16</a> .
2020-04-08	Added <a href="#">Added ability in FortiSwitch to query FortiGuard IoT service for device details on page 468</a> , <a href="#">Redesign Security Rating scorecards on page 121</a> , <a href="#">Using the root FortiGate with disk to store historic user and device information on page 49</a> , and <a href="#">Support SD-WAN integration with OCVPN on page 156</a> .



Date	Change Description
2020-04-13	Added <a href="#">FortiSwitch voice device detection on page 470</a> and <a href="#">Synchronizing objects across the Security Fabric on page 49</a> .
2020-03-31	Initial release of FortiOS 6.4.0.

# GUI

This section includes new features related to the FortiOS GUI:

- [Getting started on page 12](#)
- [Dashboards and widgets on page 16](#)

## Getting started

This section includes new features related to getting started in the FortiOS GUI:

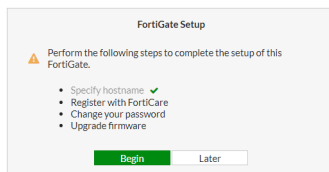
- [Firmware upgrade notifications on page 12](#)
- [Transfer a device to another FortiCloud account 6.4.1 on page 13](#)
- [FortiCare registration disclaimer 6.4.1 on page 15](#)

## Firmware upgrade notifications

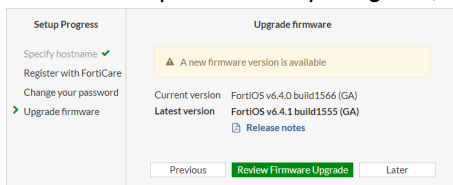
FortiGates with a firmware upgrade license and that are connected to FortiGuard display upgrade notifications in the setup window, the banner, and the FortiGate menu. You can use the CLI console to enable or disable the notifications.

**To view the firmware upgrade notifications in the GUI:**

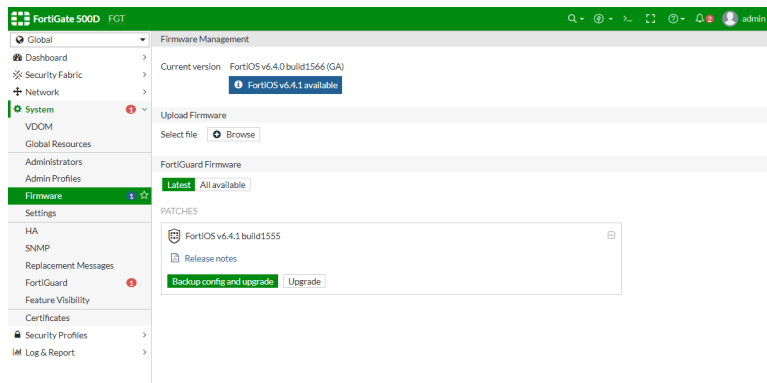
1. When you log in to FortiGate, the *FortiGate Setup* window includes an *Upgrade firmware* step. Click *Begin*.



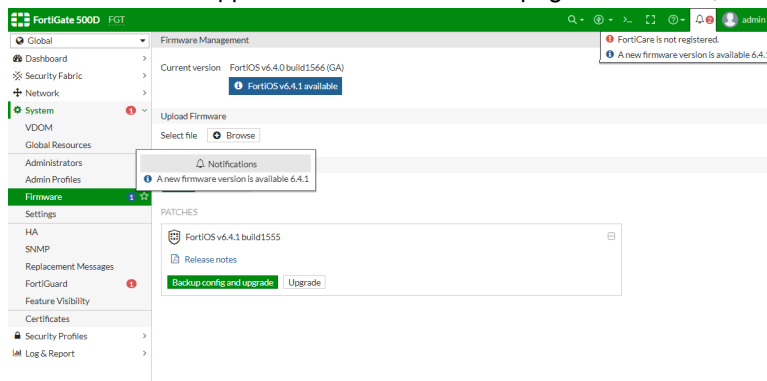
2. Follow the steps in the *Setup Progress*, then click *Review Firmware Upgrade*.



You are taken to the *Firmware* page.



3. Notifications also appear next to the *Firmware* page in the menu, and below the *Notification* icon in the banner.



### To enable or disable the firmware notification in the CLI:

```
config system global
    set gui-firmware-upgrade-setup-warning {enable | disable}
end
```

Firmware notifications are enabled by default.

## Transfer a device to another FortiCloud account - 6.4.1

Master account users can transfer a device from one FortiCloud/FortiCare account to another. Users can transfer a device up to three times within a twelve-month time period.

### Requirements:

To transfer an account, you must:

- Have access to the FortiGate, as well as both the FortiCloud and FortiCare accounts.
- Be a master account user.

To verify you are the master account user, go to [support.fortinet.com](https://support.fortinet.com). Click the user name, then click *My Account*.

**FortiCloud**  
Customer Service & Support

Home Asset Assistance Download Feedback

**Account**

Company: Fortinet  
Title: N/A  
Email: [redacted]  
Telephone: [redacted]  
Activated Since: 2013-02-19

**Account Profile**

Account Information

Phone: [redacted]  
Industry: [redacted]  
Organization Size: N/A

**Master User**

Email: [redacted]  
Name: [redacted]  
Title: N/A  
All ticket process via Email: Y  
For more information about Email interaction, please Click Here

**Edit**



You can transfer a device up to three times in a twelve-month time period. If more transfers are required within the twelve-month time period, contact [Technical Support](#) to request the transfer.

### To transfer an account in the GUI:

1. Go to *Dashboard > Status*. In the *Status* dashboard, click on *FortiCare Support*, and click *Transfer FortiGate to Another Account*.



You can also transfer an account from *System > FortiGuard*.

**FortiGate 201E B**

Global Dashboard Status

**System Information**

Hostname	B
Serial Number	[redacted]
Firmware	v6.4.0 build1613 (interim)
Virtual Domains	✓
Mode	NAT
System Time	2020/04/17 14:06:38
Uptime	00:04:09:37
WAN IP	172.18.60.92

**Licenses (192.168.100.205)**

- ✓ FortiCare Support
- ✓ Firmware
- ✓ AntiVirus
- ✓ Web Filtering
- ✓ Security Rating

VDOM: 2 / 10   FortiToken: 0 / 0

20%   0%

**FortiGate Cloud**

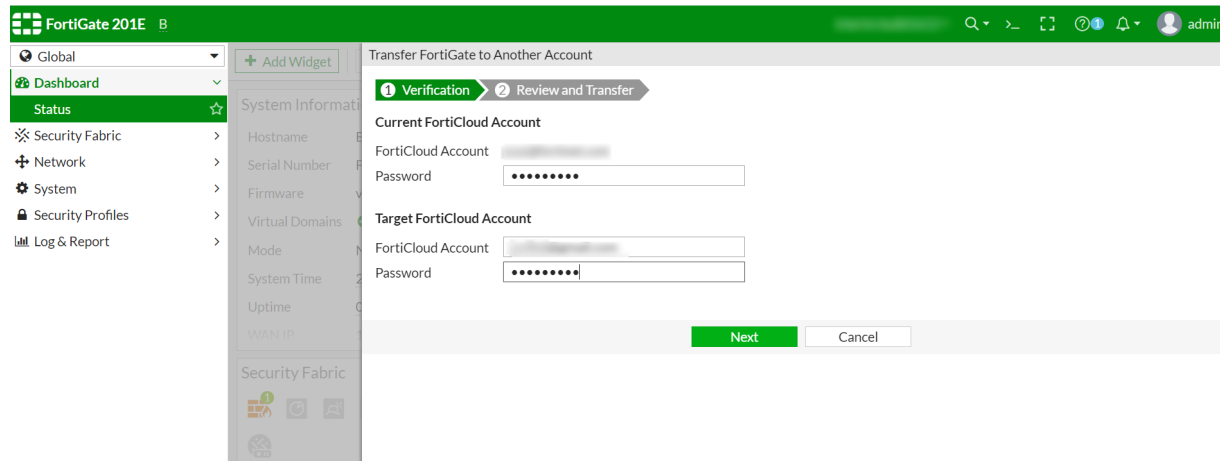
Not Activated

**Administrators**

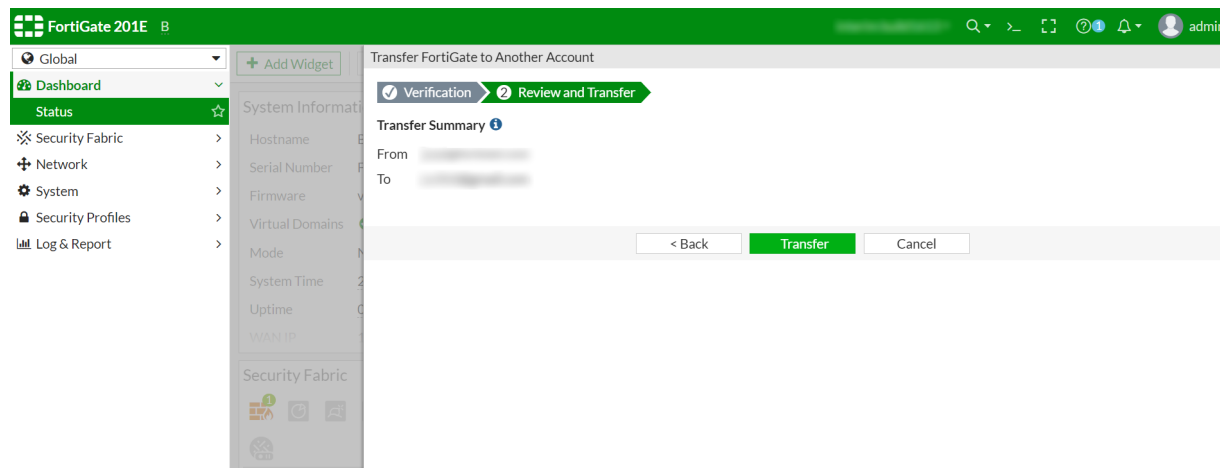
- 1 HTTPS
- 1 GUI Console
- 0 FortiExplorer

admin super\_admin

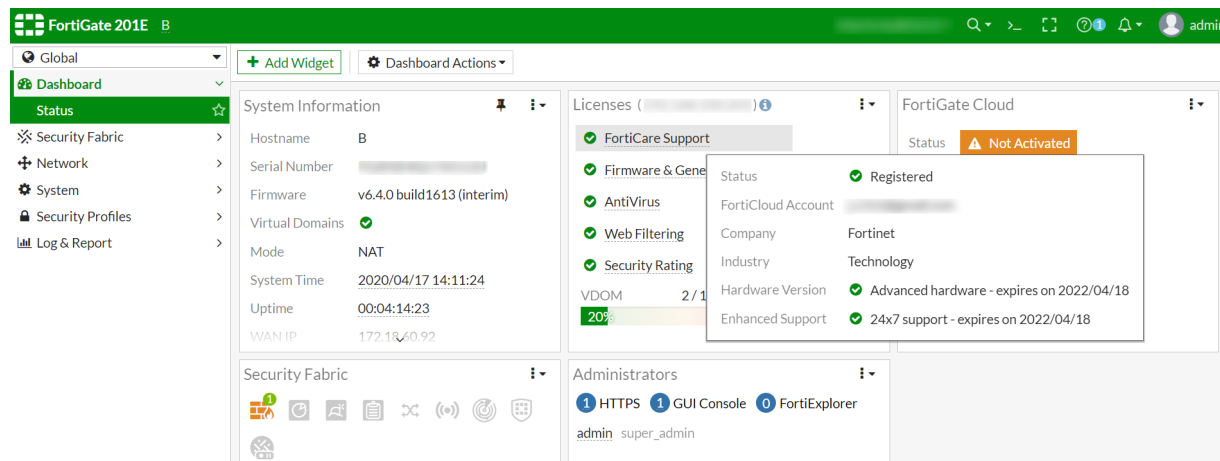
2. In the *Current FortiCloud Account* fields, enter the username and password for the current account. In the *Target FortiCloud Account* fields, enter the new username and password. Click *Next*.



FortiGate transfers the account.



After the transfer is complete, FortiGate displays the new the FortiCloud account.



## FortiCare registration disclaimer - 6.4.1

A FortiCare registration disclaimer is displayed when registering a device through the FortiGate GUI.

The following disclaimer is displayed once all information is entered in the registration page:

B: FortiCare Registration

Fortinet Product Registration Agreement  
 Fortinet Service Terms & Conditions  
 For FortiCare, FortiGuard and other Service Offerings

THESE TERMS AND CONDITIONS APPLY TO THE PROVISION OF SERVICES BY FORTINET AND EXCLUSIVELY GOVERN THE LEGAL RELATIONSHIP BETWEEN YOU (THE CUSTOMER) AND FORTINET. IT SETS FORTH THE LEGALLY BINDING RIGHTS AND OBLIGATIONS OF THE CUSTOMER IN RELATION TO FORTICARE SUPPORT OR FORTIGUARD SUBSCRIPTION SERVICES OR OTHER FORTINET SERVICE OFFERINGS. THE CUSTOMER CONSENTS TO BE BOUND BY THESE TERMS AND CONDITIONS AND TO HAVE BECOME PARTY TO THIS "AGREEMENT" (THIS OR THE "AGREEMENT") AND REPRESENTS TO HAVE READ AND UNDERSTOOD THIS AGREEMENT AND HAVE HAD SUFFICIENT OPPORTUNITY TO CONSULT WITH COUNSEL BEFORE AGREEING TO THE TERMS HEREIN. THE CUSTOMER AGREES THAT ANY OF THE FOLLOWING ACTIONS BY CUSTOMER REPRESENTATIVES REPRESENT THE CUSTOMER'S AUTHORIZED CONSENT TO BE BOUND BY THIS AGREEMENT: (I) RECEIVING, DOWNLOADING, DEPLOYING OR USING ANY SOFTWARE PROVIDED IN CONNECTION WITH FORTINET SERVICES, (II) RECEIVING, CONFIGURING, LOGGING IN, REGISTERING OR OTHERWISE USING OR BENEFITTING FROM THE SERVICES, OR (III) BY CLICKING ON THE "ACCEPT" BUTTON UPON REGISTRATION (ANY OF (I), (II), OR (III) SHALL CONSTITUTE "ACCEPTANCE" BY CUSTOMER). THE CUSTOMER HEREBY ACKNOWLEDGE AND AGREES THAT THE PERSON ENGAGING IN (I), (II), AND/OR (III) IS AUTHORIZED TO BIND THE CUSTOMER TO THE TERMS HEREIN. FOR CLARITY, NOTWITHSTANDING ANYTHING TO THE CONTRARY, IF CUSTOMER IS USING AN AUTOREGISTRATION TOOL, CUSTOMER ACKNOWLEDGES AND AGREES THAT ANY AND ALL UNITS REGISTERED USING SUCH TOOL SHALL BE SUBJECT TO THESE TERMS AND CONDITIONS.

Services are available independently or in connection with the purchase of Fortinet's commercial networking products and related equipment, including hardware products with embedded software, and software products sold and licensed to you pursuant to Fortinet's End User License Agreement ("EULA"), which EULA is available at <https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf>, and you hereby agree to the terms of the EULA.

This Agreement and the Sales Order Acknowledgment represent a legal agreement between the parties with respect to FortiCare and FortiGuard Subscription services or other Fortinet services, and shall supersede all prior representations, discussions, negotiations and agreements, whether written or oral. This document expressly supersedes the Customer Service & Support Reference Guide (CSS Reference Guide) and all other service descriptions, and notwithstanding anything to the contrary, Fortinet is only bound by, and Customer is only entitled to, services pursuant to

☐ I agree to the FortiCloud terms & conditions

Previous OK Cancel

The user must select the checkbox to agree to the terms and conditions in order to complete the registration.

## Dashboards and widgets

This section includes new features related to dashboards and widgets:

- [Consolidate Monitor and FortiView pages on page 16](#)
- [IP address tooltips on page 22](#)
- [View session information for a compromised host 6.4.1 on page 24](#)
- [Consolidated dashboard usability improvements 6.4.1 on page 25](#)
- [Add detachable CLI console tabs 6.4.2 on page 31](#)
- [Implement a user device store to centralize device data 6.4.3 on page 32](#)

## Consolidate Monitor and FortiView pages

The Monitoring & FortiView consoles were removed from the tree menu and now appear as widgets in the Dashboards menu. The dashboard navigation has been improved for easy access to features such as creating a new dashboard. New widgets were added to the Add Widget menu to create custom dashboards.

### Improved navigation and functionality

Dashboard options are now located in the dashboard banner for easier access and visibility. Users can use a widget to create a standalone dashboard.

### New WiFi health monitor

- The existing WiFi Health Monitor widgets were consolidated into a new default WiFi dashboard in the tree menu. This dashboard contains the following widgets:
- FortiAP Status
- Channel Utilization
- Clients By FortiAP
- Signal Strength
- Rogue APs
- Historical Clients
- InterfereAPs
- Login Failures

### New network monitor

A new Network dashboard was added to the tree menu. This dashboard contains the following widgets:

- Routing Monitor
- DHCP Monitor
- SD-WAN Monitor
- IPsec Monitor
- SSL-VPN Monitor

### Consolidated Formative menu

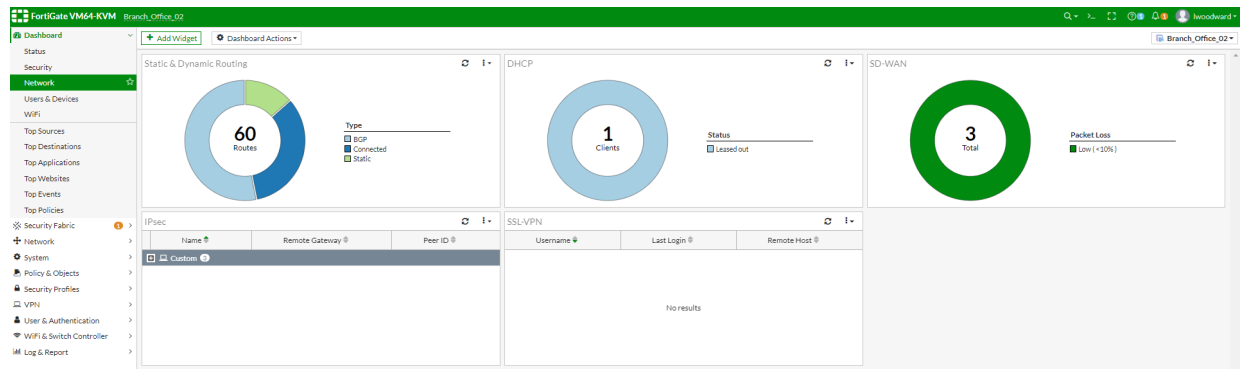
The FortiView module has been consolidated into dashboard widgets. The sections of the FortiView module that were not incorporated into widgets were moved to the Log & Reports module in the tree menu. The Threat Map was removed from the GUI.

The following FortiView widgets were created:

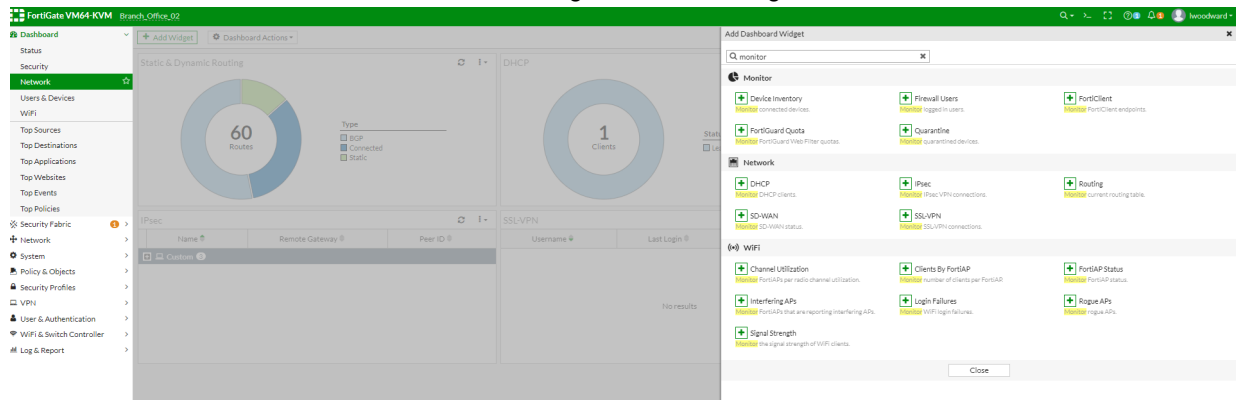
- FortiClient
- Firewall users
- Quarantine

### To add a widget to a dashboard:

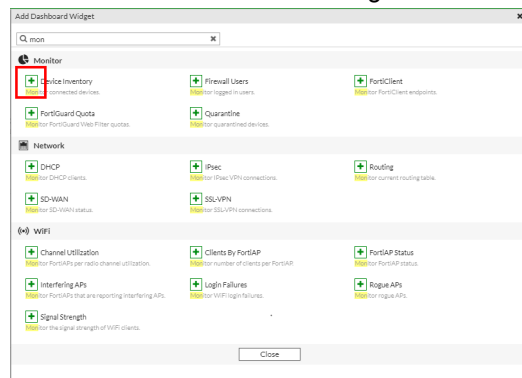
1. Open a dashboard in the tree menu.
2. In widget banner, click *Add Widget*. The *Add Dashboard Widget* window opens. The widgets are organized by category.



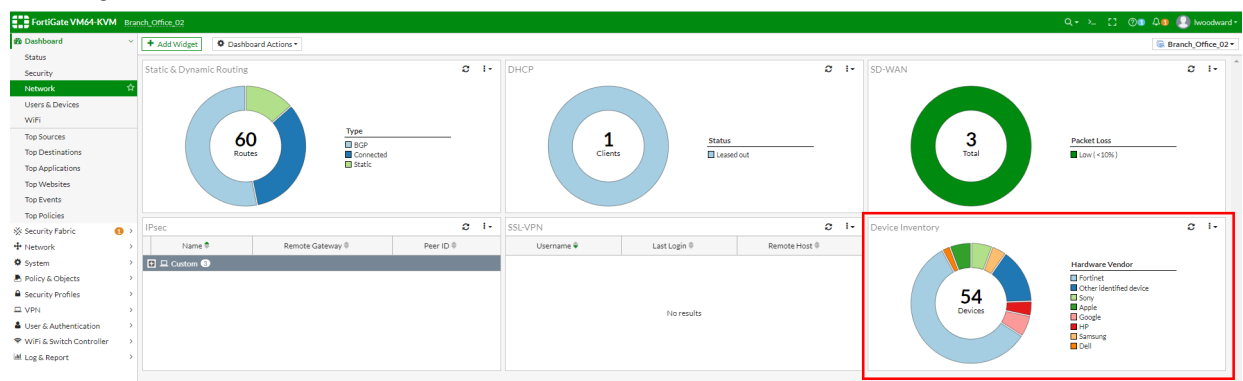
3. Enter a search term in the **Search** field to find a widget, or scroll through the window.



4. Click the **Add** icon to add the widget to the dashboard.



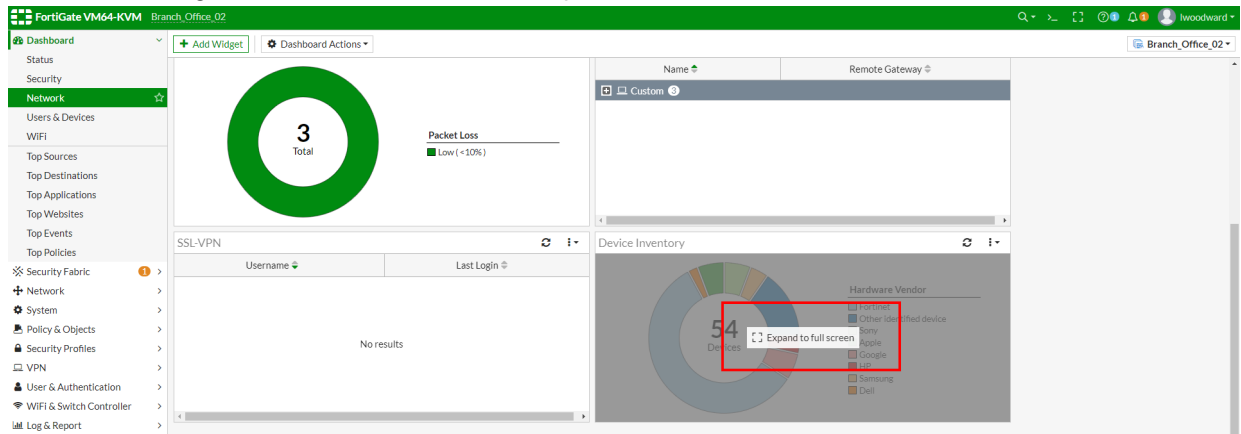
The widget is added to the dashboard.



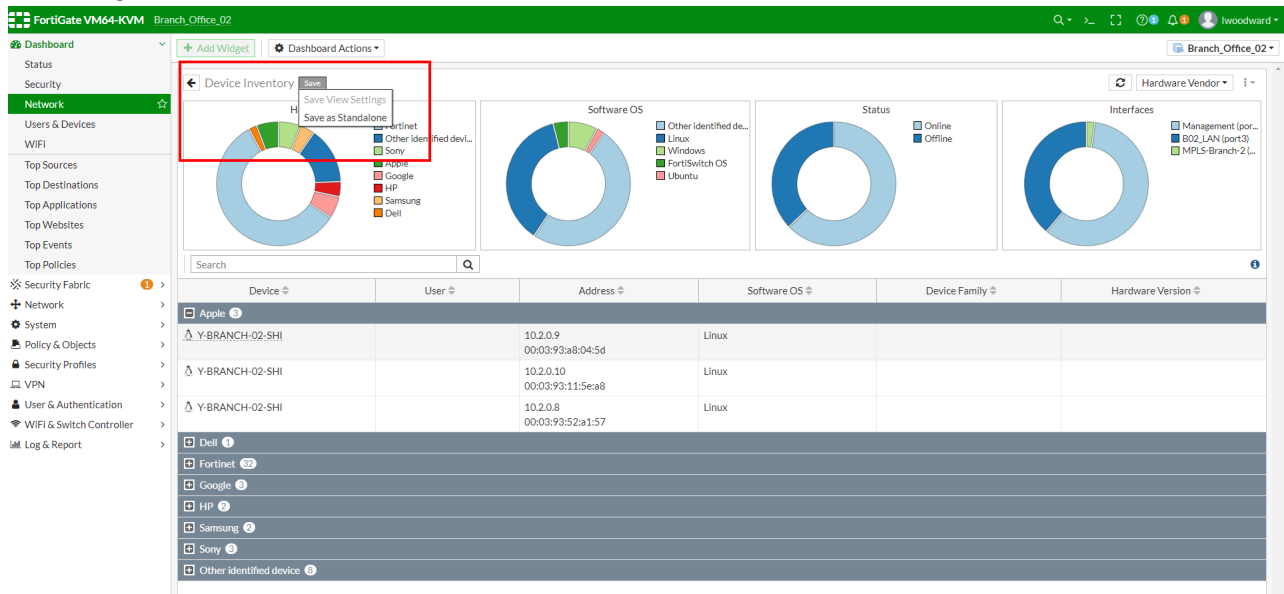


## To create a dashboard with a widget:

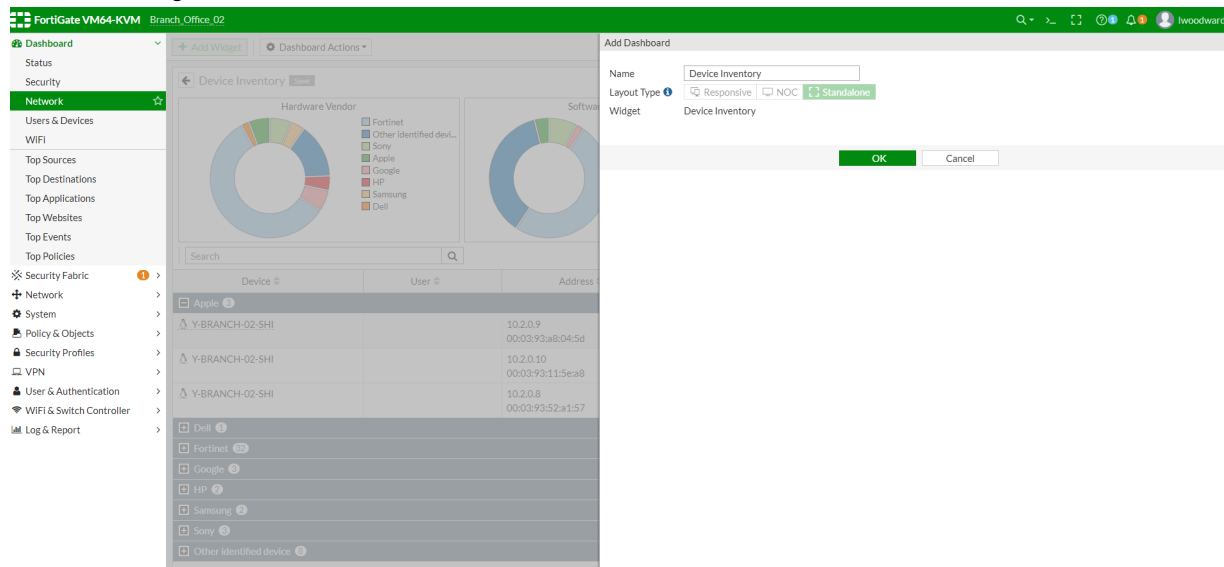
1. Hover over a widget in the dashboard, and click *Expand to Full Screen*.



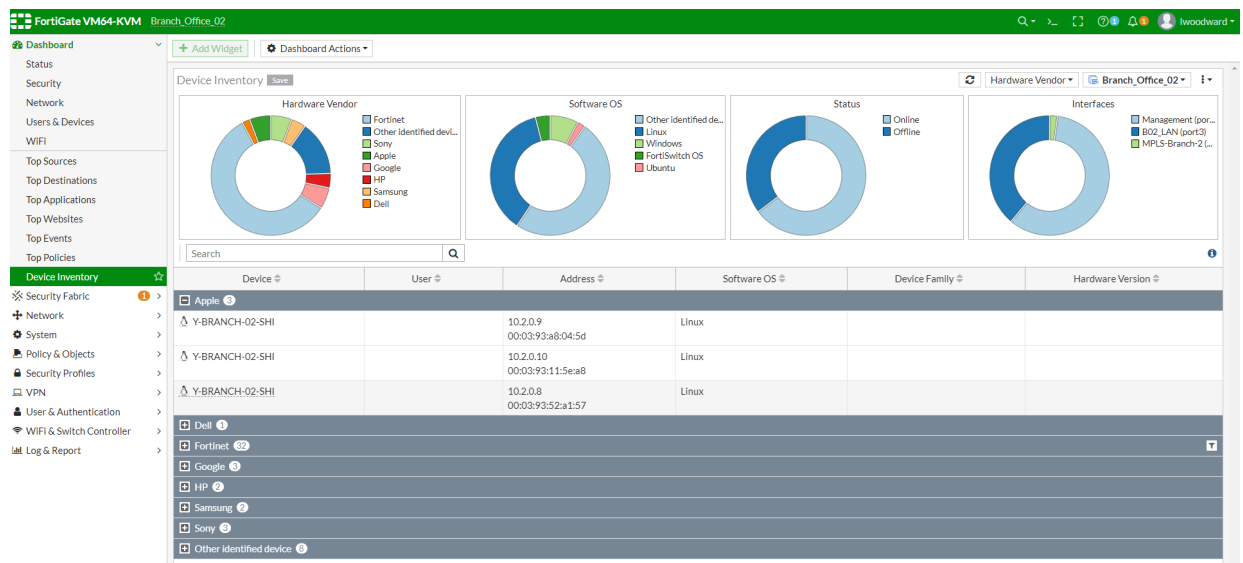
2. In the widget banner, click *Save > Save as Standalone*.



3. In the *Add Widget* window, click *OK*.

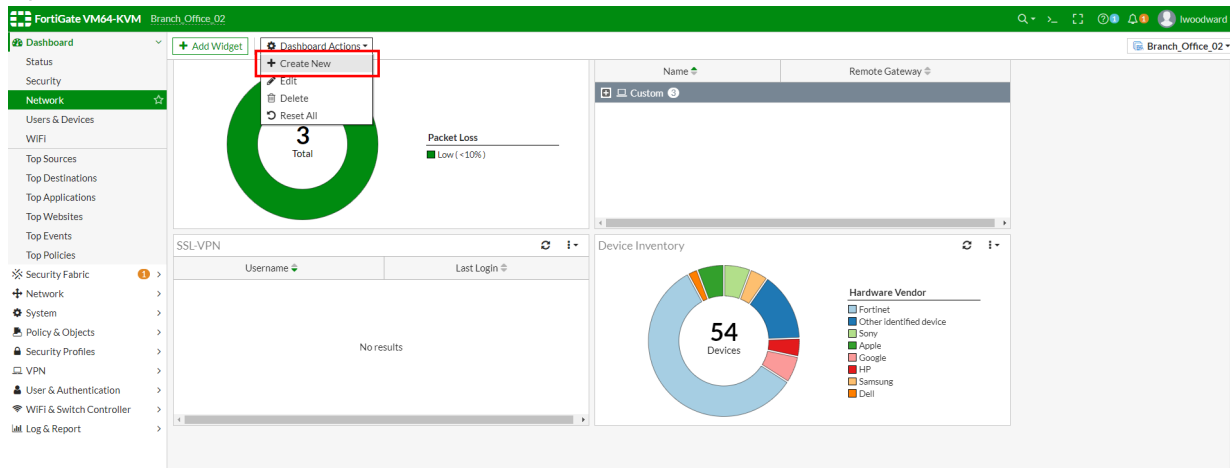


The new dashboard is added to the tree menu.

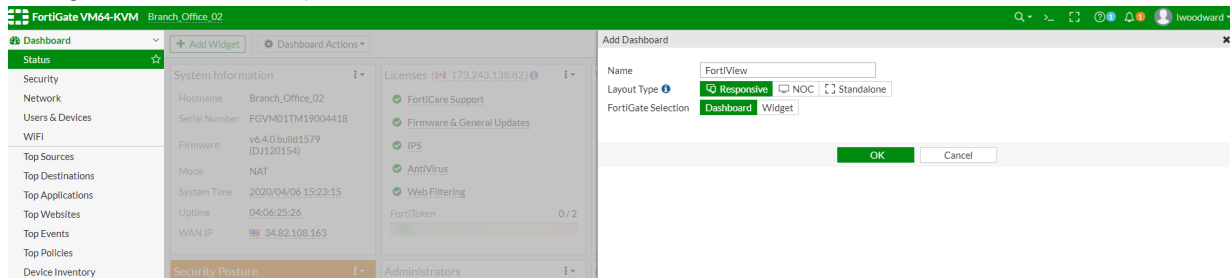


## To create a new custom dashboard:

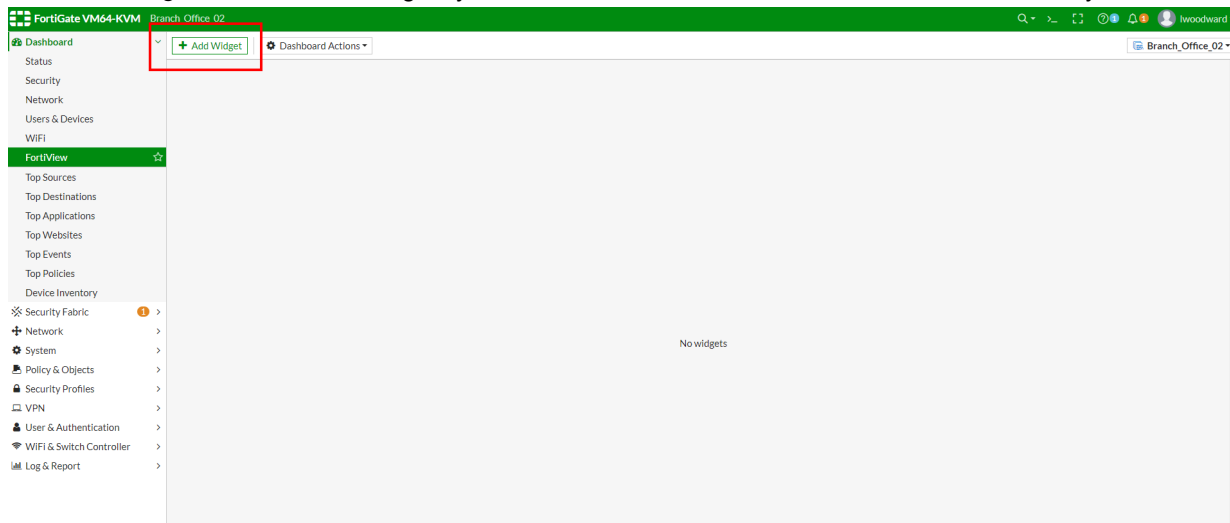
1. Open a dashboard, and click *Dashboard Actions > Create New*.



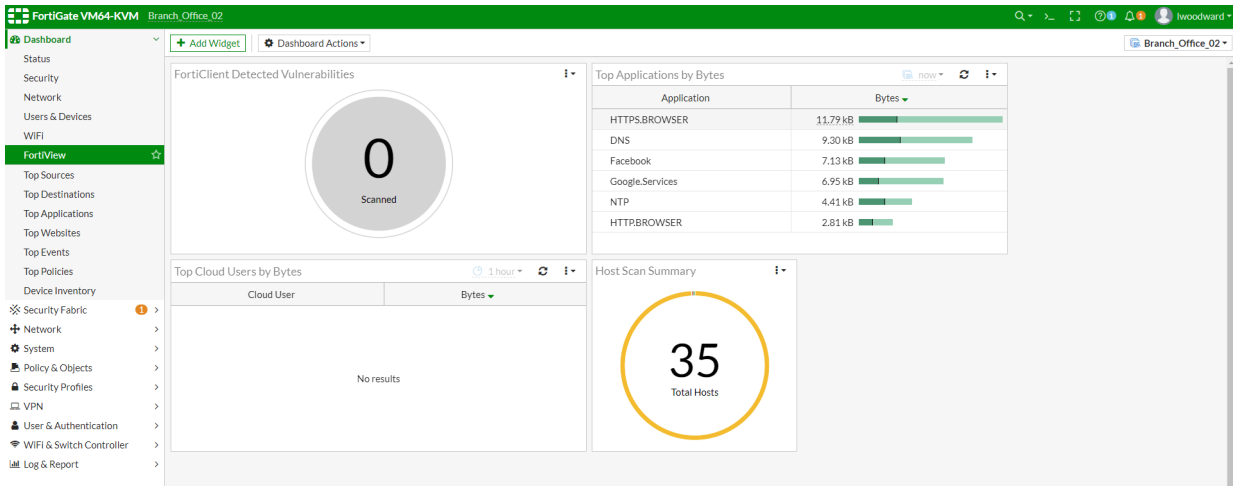
2. Configure the dashboard options, and click *OK*. The dashboard is added to the tree menu.



3. Click *Add Widget* and select the widgets you want to add to the new dashboard. Click *Close* when you are done.



The widgets are added to the dashboard.

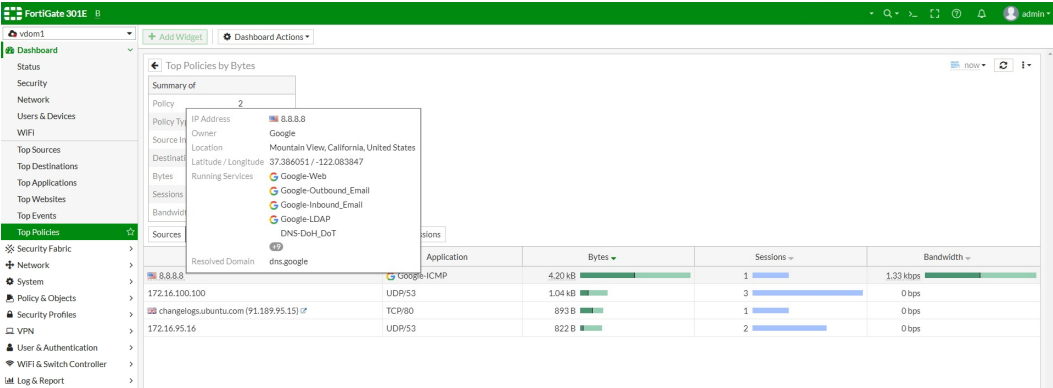


## IP address tooltips

Hovering over an IP address on different GUI pages (for example, *Dashboard > Top Policies*, *Log & Report > Forward Traffic*, *Security Fabric > External Connectors*) displays a tooltip that contains additional information about the IP such as its country, location, owner, resolved domains, and internet services.

### Tooltip examples

*Dashboard > Top Policies* page:

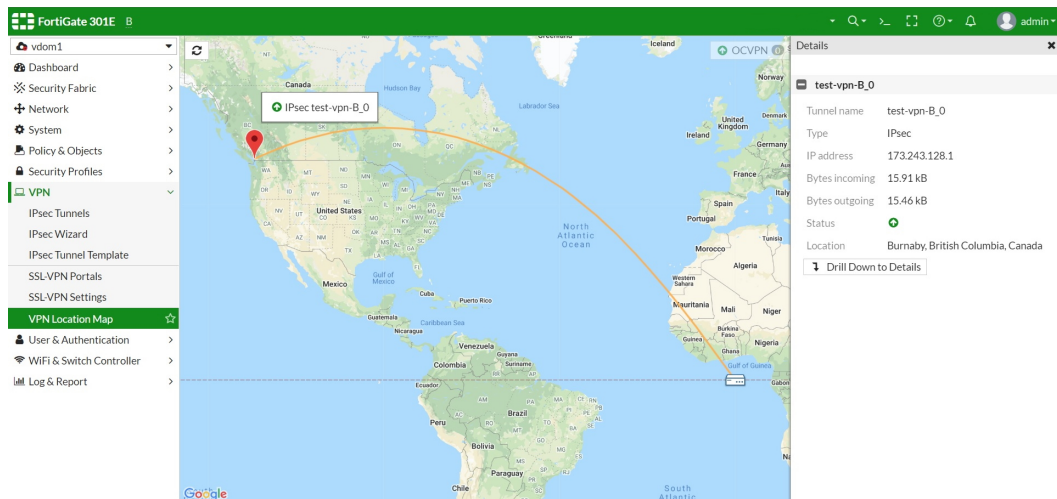


*Log & Report > Forward Traffic* page:

FortiGate 301E B										vdom1										Policy UUID: 79177b1a-d626-51ea-ea53-7784269c1c49										Add Filter										Details										B																																																																																																																																	
Dashboard										Security Fabric										Network										System										Policy & Objects										Security Profiles										VPN										User & Authentication										Log & Report										Forward Traffic										Local Traffic										Multicast Traffic										Sniffer Traffic										Events										AntiVirus										Web Filter										SSL										DNS Query									
Source										Device										Destination										Application Name										Result										Policy										Policy Name										Policy Type																																																																																																													
2.2.2.1										704ca5:97:d9:26										172.16.95.16																				172 B / 341 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										2001:569:2::cf2:af1a (ctldlwin										IP Address										2001:569:2::cf2:af11										B / 225 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																			
2001:10:2:2:1										704ca5:97:d9:26										2001:569:2::cf2:af20 (ctldlwin										Location										Canada										2 B / 356 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																			
2001:10:2:2:1										704ca5:97:d9:26										52.148.151.26 (settings-win.dat										Latitude / Longitude										60 / -116										2 B / 356 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																			
2001:10:2:2:1										704ca5:97:d9:26										2001:569:2::cf2:af11 (ctldl.windowsupdate.com)										Resolved Domain										ctldl.windowsupdate.com										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				212 B / 356 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													
2001:10:2:2:1										704ca5:97:d9:26										172.16.100.100																				124 B / 281 B										Test_Policy_2 (2)										Test_Policy_2										Firewall																																																																																																													

Network > DNS page:

VPN > VPN Location Map page:



## View session information for a compromised host - 6.4.1

You can use the *Top Compromised Hosts by Verdict* widget to view the session information for a compromised host.

To view session information for a compromised host in the GUI:

1. Go to *Dashboard > Security* and expand the *Top Compromised Hosts by Verdict* widget.

Source	Device	Verdict	Threats
10.200.1.21	LAN-FSW-GUEST	Compromised	1
10.100.92.5	LAN-FSW-GUEST	Compromised	1
10.200.1.19	LAN-FSW-GUEST	Compromised	1
10.100.92.5	LAN-FINANCE	Compromised	1
10.200.1.20	LAN-FSW-GUEST	Compromised	1
10.100.92.15	LAN-FINANCE	Compromised	1
10.200.1.5	LAN-FSW-GUEST	Compromised	1
10.200.1.17	LAN-FSW-GUEST	Compromised	1
10.200.1.3	LAN-FSW-GUEST	Compromised	1
10.200.1.16	LAN-FSW-GUEST	Compromised	1
10.200.1.15	LAN-FSW-GUEST	Compromised	1
10.200.1.13	LAN-FSW-GUEST	Compromised	1
10.200.1.14	LAN-FSW-GUEST	Compromised	1
10.200.1.18	LAN-FSW-GUEST	Compromised	1
10.200.1.4	LAN-FSW-GUEST	Compromised	1
10.200.1.2	LAN-FSW-GUEST	Compromised	1
10.200.1.8	LAN-FSW-GUEST	Compromised	1
10.200.1.9	LAN-FSW-GUEST	Compromised	1
10.200.1.6	LAN-FSW-GUEST	Compromised	1
10.200.1.10	LAN-FSW-GUEST	Compromised	1
10.200.1.12	LAN-FSW-GUEST	Compromised	1
10.200.1.11	LAN-FSW-GUEST	Compromised	1
10.200.1.7	LAN-FSW-GUEST	Compromised	1
10.100.91.100	TAMIGERBER	Compromised	2

2. Double-click a compromised host to view the session information. You can also right-click a compromised host, and select *View Sessions*.

**Top Compromised Hosts by Verdict**

Summary of

10.100.91.100 **Critical Risk**

Device: TAMIGERBER

Verdict: Compromised

Threats: 2

FortiGate: fshuva-slx4one

Actions: [Dropdown]

Detected Pattern	Threat Type	Threat Name	Threat Category	Detect method	Events	Security Action	Web Category
103.226.154.43	Malware	CnC	View Sessions	infected-ip	5	timeout	Malicious Websites
103.226.154.43	Malware	CnC		infected-ip	1	dropped	Malicious Websites
103.226.154.43	Malware	CnC		infected-ip	1	timeout	Malicious Websites

3. Double-click a session, or right-click the session and select *View Sessions* to view the information.

**Top Compromised Hosts by Verdict**

Summary of

10.100.91.100 **Critical Risk**

Device: TAMIGERBER

Verdict: Compromised

Threats: 2

FortiGate: fshuva-slx4one

Actions: [Dropdown]

Blacklist | Suspicious | **Sessions**

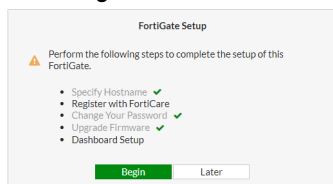
Date/Time	Source	Destination	Application Name	Security Action	Sent / Received
2020/05/21 03:45:03	10.100.91.100	103.226.154.43	HTTP		152 B / 0 B
2020/05/21 03:40:03	10.100.91.100	103.226.154.43	HTTP		152 B / 0 B
2020/05/21 03:35:03	10.100.91.100	103.226.154.43	HTTP		152 B / 0 B
2020/05/21 03:30:04	10.100.91.100	103.226.154.43	HTTP		152 B / 0 B
2020/05/21 03:24:34	10.100.91.100	103.226.154.43	HTTP		152 B / 0 B

## Consolidated dashboard usability improvements - 6.4.1

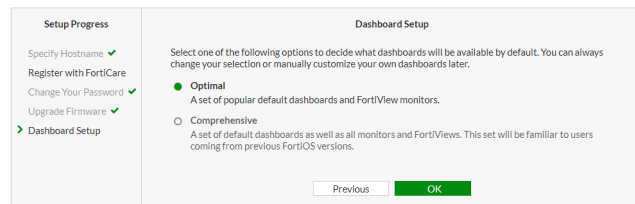
A *What's New in FortiOS 6.4* video appears after upgrade to highlight new features such as Dashboard and Monitor usage. Two modes, *Optimal* and *Comprehensive*, were added to display different default monitors. Users can also easily add new Dashboards or Monitors directly from the menu.

### To select a dashboard template at log in:

1. Log in to FortiGate. The *Dashboard Setup* option appears in the *FortiGate Setup* dialog.
2. Click *Begin*.



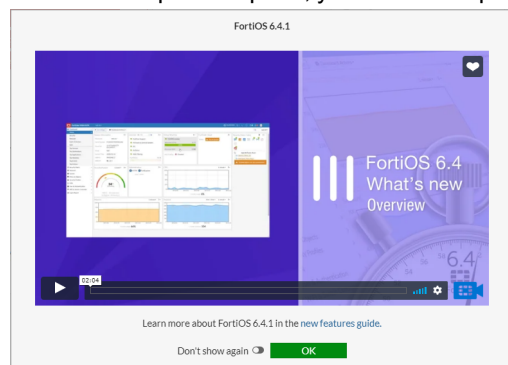
3. At the *Dashboard Setup* step, select *Optimal* or *Comprehensive* dashboard template.



The following dashboards and monitors are included in the default templates:

<b>Optimal</b>	Dashboard	Status, Security, Network, Users & Devices, WiFi
	Monitor	FortiView Sources, FortiView Destinations, FortiView Applications, FortiView Web Sites, FortiView Policies, FortiView Sessions
<b>Comprehensive</b>	Dashboard	Status, WiFi
	Monitor	FortiView Sources, FortiView Destinations, FortiView Applications, FortiView Web Sites, FortiView Threats, FortiView Compromised Hosts, FortiView Policies, FortiView Sessions, Device Inventory Monitor, Routing Monitor, DHCP Monitor, SD-WAN Monitor, FortiGuard Quota Monitor, IPsec Monitor, SSL-VPN Monitor, Firewall User Monitor, Quarantine Monitor, FortiClient Monitor, FortiAP Clients Monitor, Rogue APs Monitor

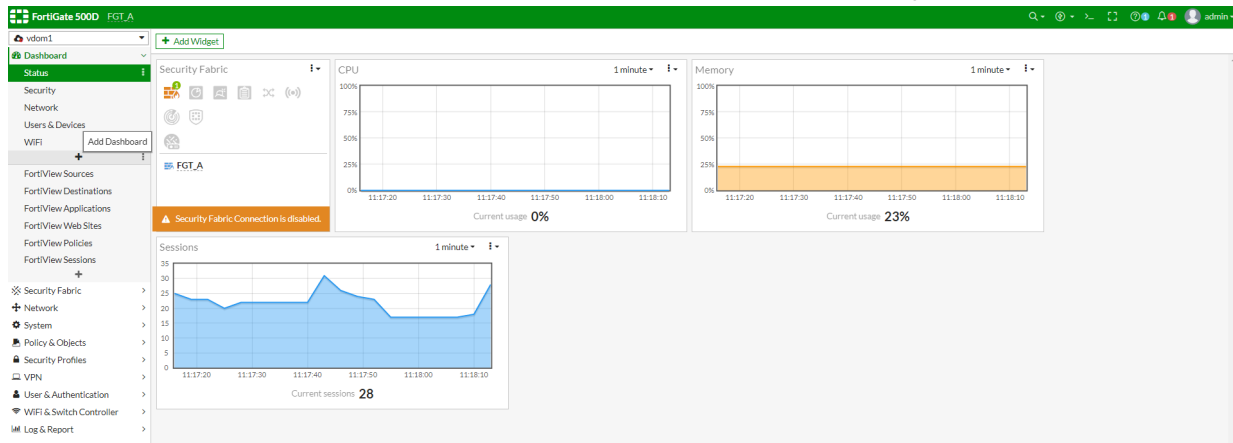
4. After the setup is complete, you have the option to watch video about new features in FortiOS 6.4.1.



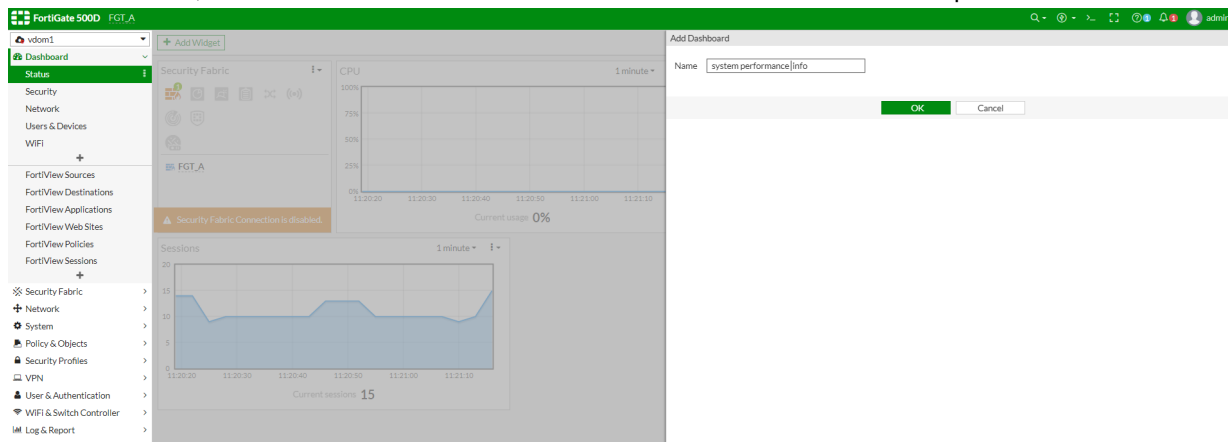


## To add a dashboard with the GUI:

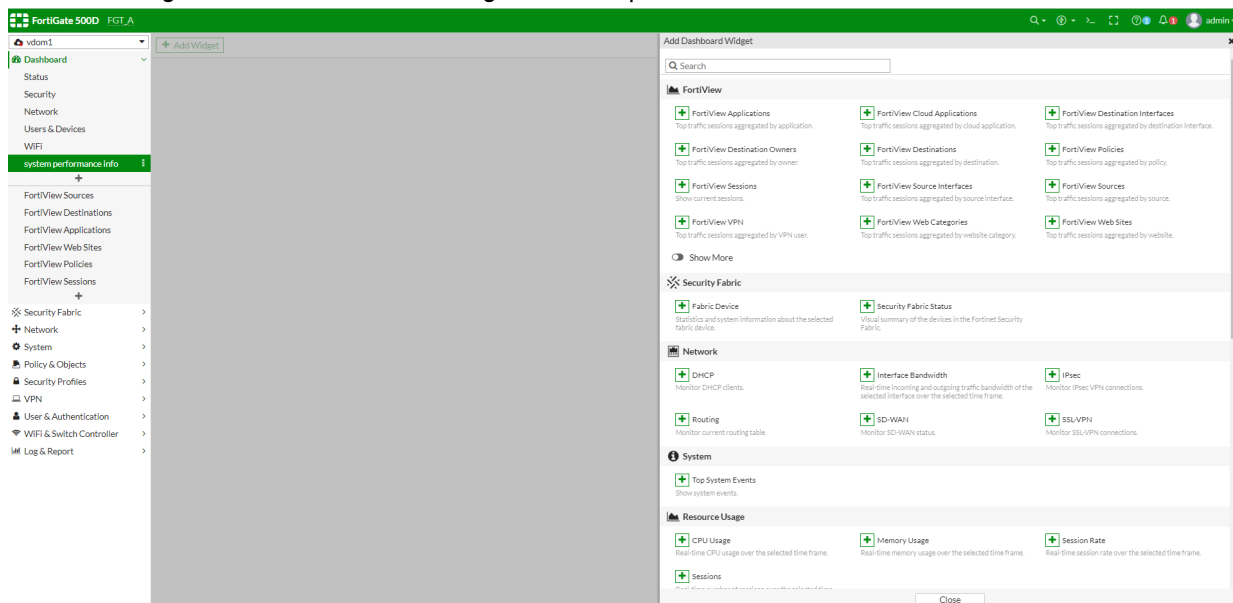
1. Under **Dashboard**, click the **Add Dashboard** button. The **Add Dashboard** window opens.



2. In the **Name** field, enter a name for the dashboard and click **OK**. The new dashboard opens.



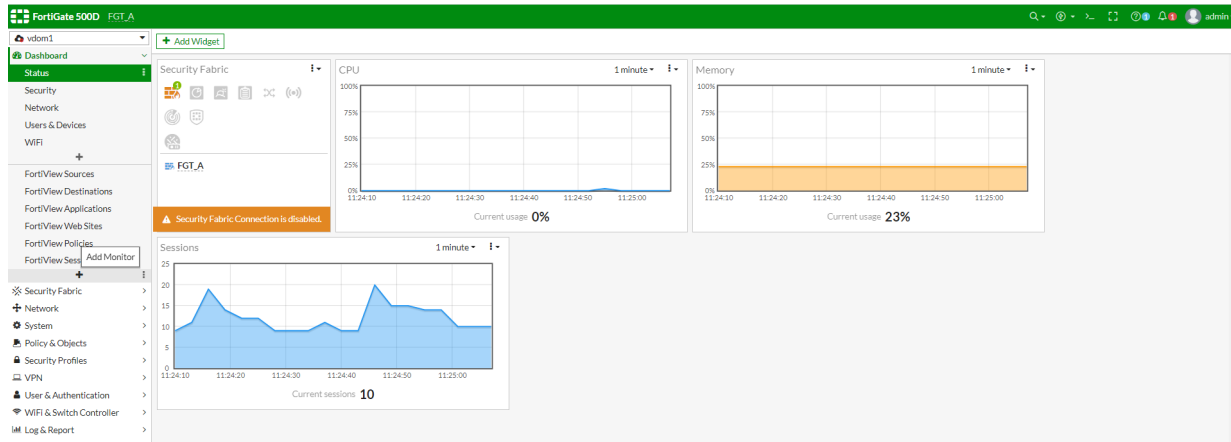
3. Click **Add Widget**. The **Add Dashboard Widget** window opens.



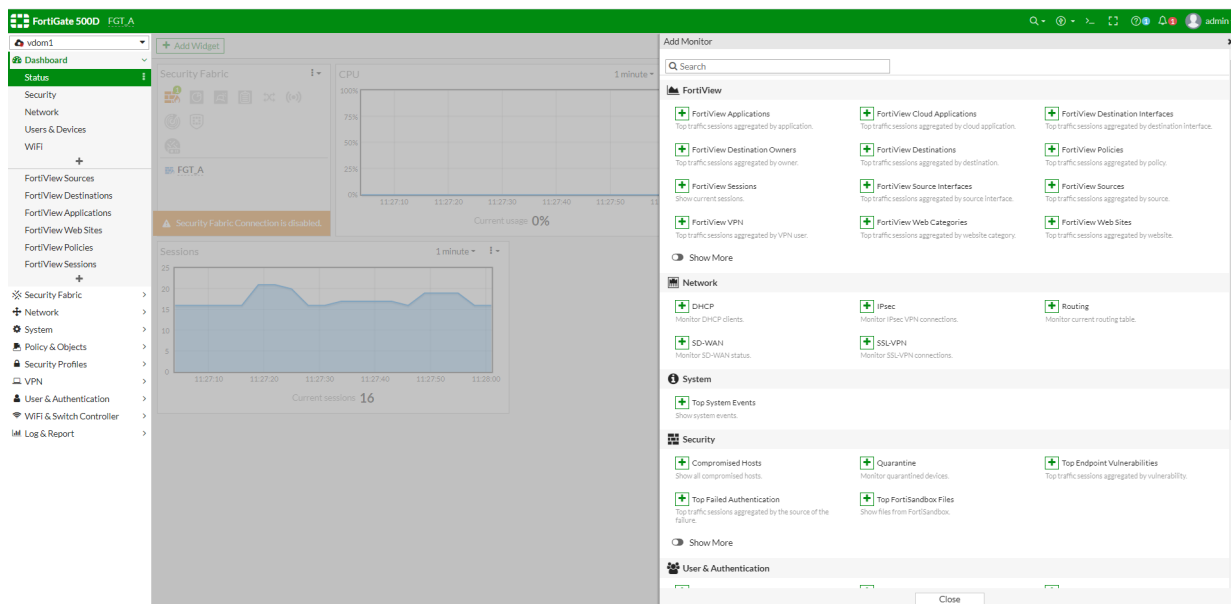
- Click the **Add** button next to the widget and configure the widget settings. You can add more than one widget at a time.
- Click **Close**.

### To add a monitor with the GUI:

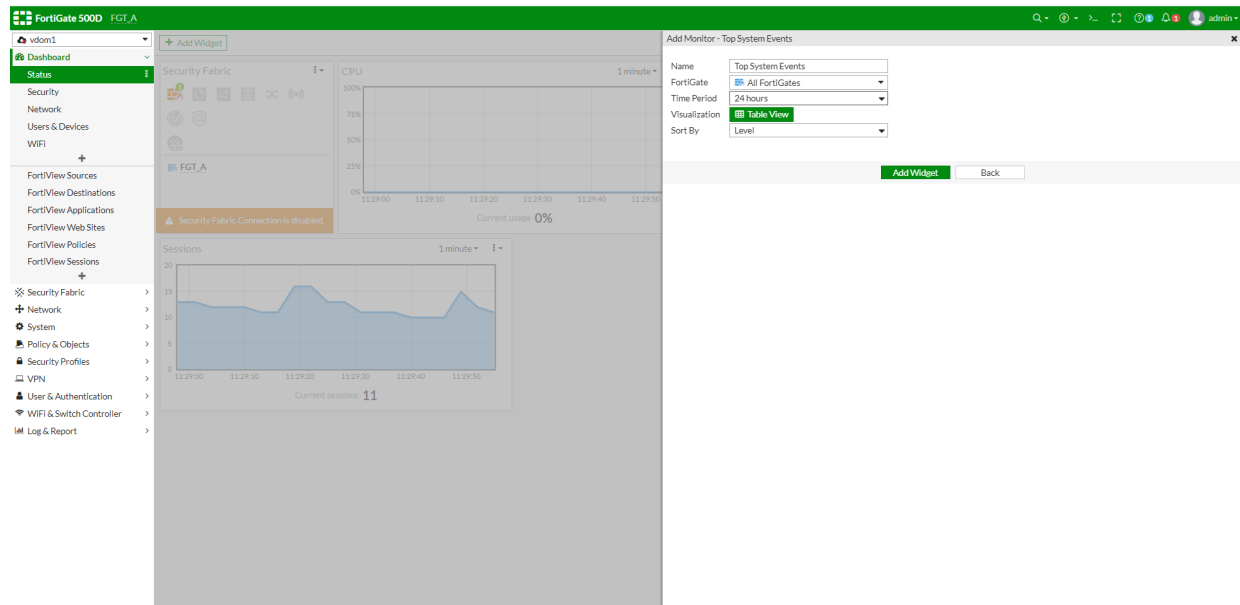
- Click the **Add Monitor** button. The **Add Monitor** window opens.



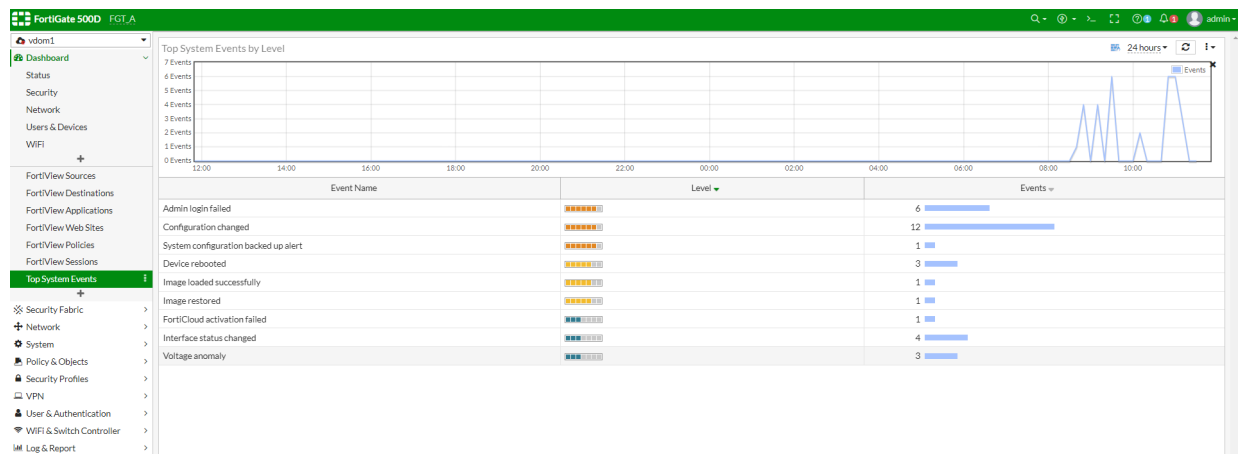
- Click the **Add** button next a monitor.



### 3. Configure the monitor settings.

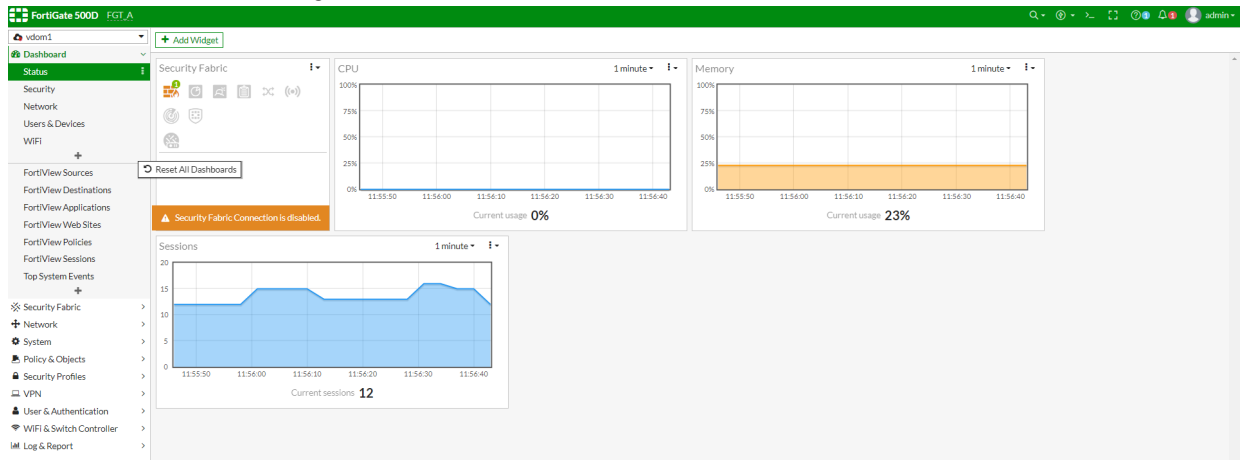


The monitor is added to the tree menu.

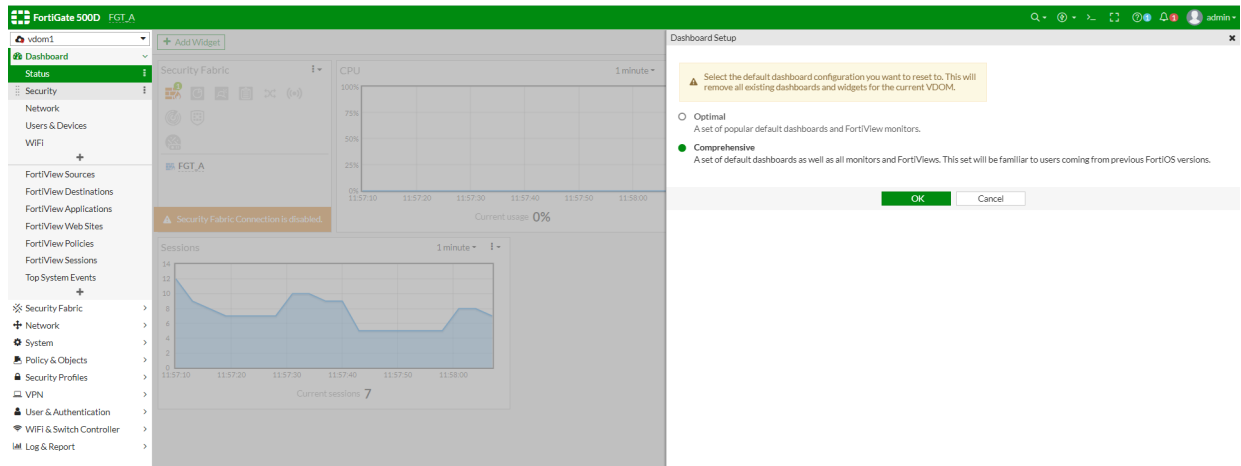


## To change the dashboard from Optimal to Comprehensive view with the GUI:

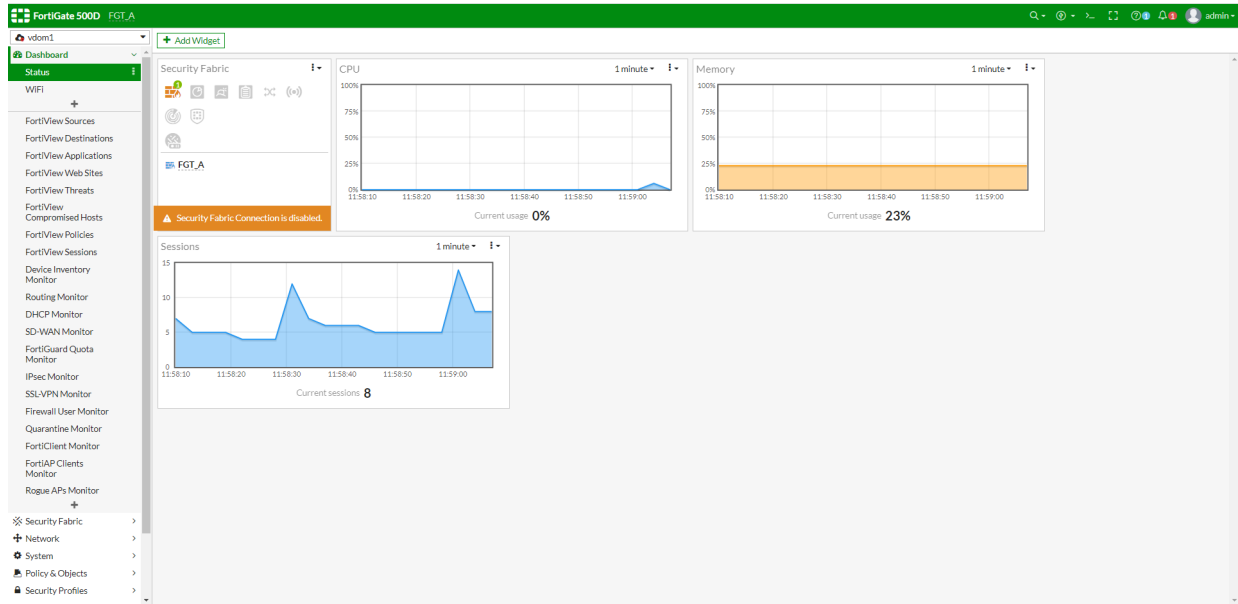
1. Click the menu icon at the right side of the *Add Dashboards* or *Add Monitors* button and click *Reset all Dashboards*.



2. Select *Comprehensive* and click *OK*.



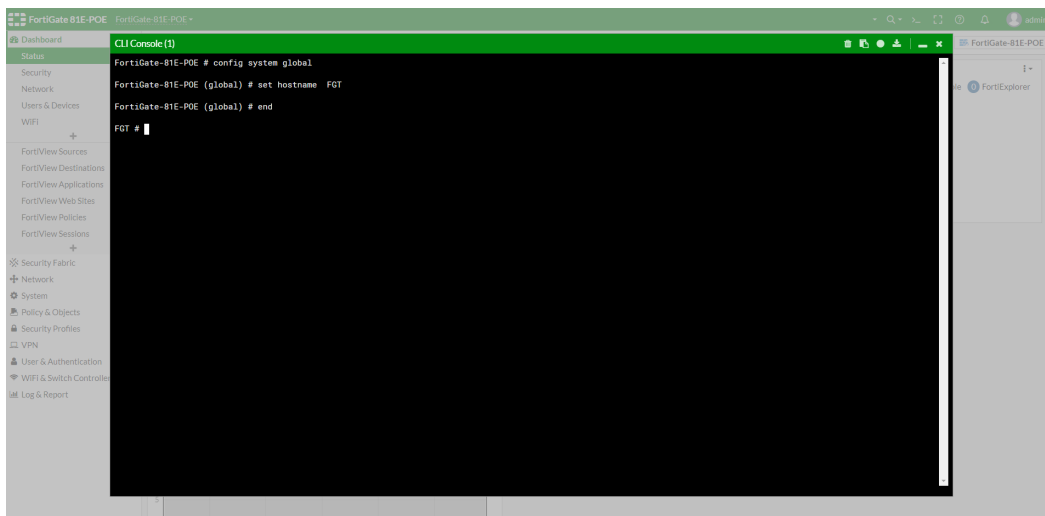
The default template is updated in the tree menu.



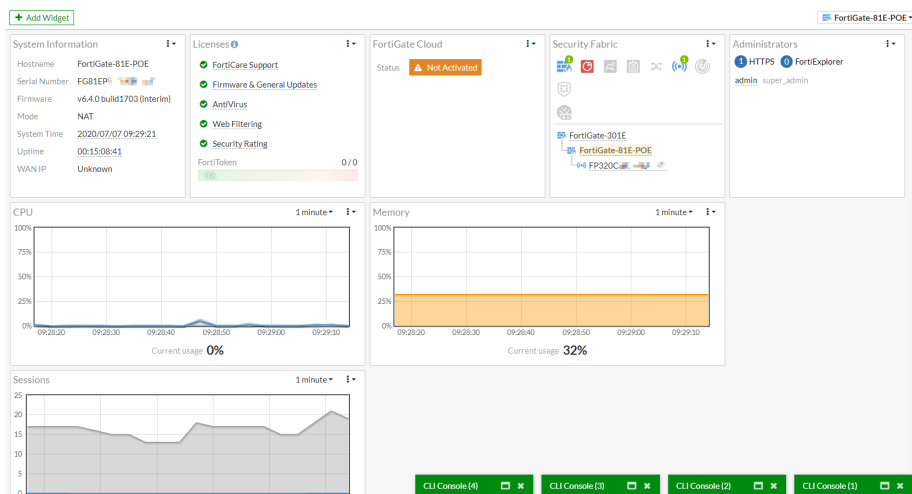
## Add detachable CLI console tabs - 6.4.2

The slide-out CLI terminal has been replaced with a full-page masking terminal. Administrators can open multiple CLI consoles, which can be minimized.

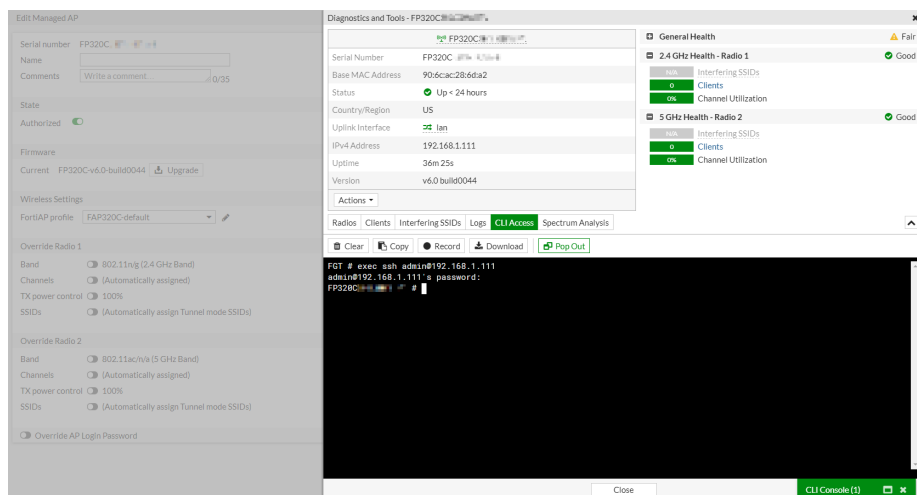
### Sample full-page CLI terminal:



## Multiple CLI consoles open and minimized:



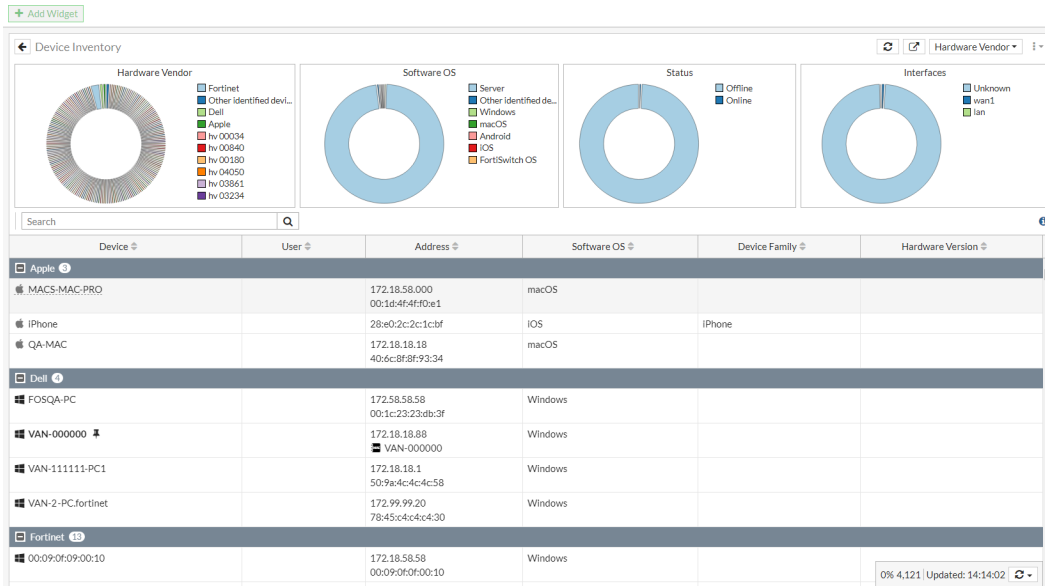
## FortiAP embedded CLI terminals have a pop out option:



## Implement a user device store to centralize device data - 6.4.3

Device data collected from different daemons is centralized in a user device store for quick access and performance. Thousands of devices can be displayed in the GUI in seconds. The maximum number of devices and users that are stored in the database can be configured.

For example, go to *Dashboard > Users & Devices* and expand the *Device Inventory* widget.



### To configure the maximum number of devices and users that are stored in the database:

```
config system global
    set user-device-store-max-devices <value>
    set user-device-store-max-users <value>
end
```

### To view the user or device on disk session information:

- List all records:
 

```
diagnose user-device-store {device | user} disk list
```
- Query by SQL WHERE clause:
 

```
diagnose user-device-store {device | user} disk query <SQL WHERE clause>
```

### To view the user or device in memory session information:

- List all records:
 

```
diagnose user-device-store {device | user} memory list
```
- Query by username or IP address:
 

```
diagnose user-device-store {device | user} memory query {ip | username} <value>
```

# Security Fabric

This section includes information about Security Fabric new features:

- [Fabric settings on page 34](#)
- [SDN connectors on page 71](#)
- [Automation stitches on page 99](#)
- [Security ratings on page 120](#)

## Fabric settings

This section includes information about Security Fabric settings related new features:

- [Integrate FortiAnalyzer management into the Security Fabric using SAML SSO on page 34](#)
- [Simplify FortiClient EMS setup on page 37](#)
- [Simplify the synchronization of EMS tags and configurations on page 40](#)
- [Allow FortiNAC to join the Security Fabric on page 42](#)
- [Redesign Fortinet Fabric Connectors and Fabric setup pages on page 44](#)
- [Display endpoints in Topology using donut chart on page 47](#)
- [Using the root FortiGate with disk to store historic user and device information on page 49](#)
- [Synchronizing objects across the Security Fabric on page 49](#)
- [Streamlined Fortinet Security Fabric setup between FortiGates 6.4.2 on page 53](#)
- [Use an FQDN in FortiSandbox fabric connectors 6.4.2 on page 55](#)
- [FortiMail Security Fabric integration 6.4.2 on page 56](#)
- [Allow EMS Cloud configuration only when the entitlement is verified 6.4.3 on page 60](#)
- [Improvements to synchronizing objects across the Security Fabric 6.4.4 on page 62](#)
- [Detect FortiManager Cloud account level subscription 6.4.4 on page 69](#)

## Integrate FortiAnalyzer management into the Security Fabric using SAML SSO

When a FortiGate is configured as the SAML SSO IdP, FortiAnalyzer can register itself as the SP (FortiAnalyzer must be running version 6.4.0). Once registered, FortiAnalyzer will be added automatically to the Security Fabric navigation in FortiOS. A similar dropdown navigation is displayed in FortiAnalyzer where users can navigate to the FortiGate using SAML SSO.

The following example assumes the root FortiGate (FGTA-1, server address 172.17.48.225:4431) has been configured as the SAML SSO IdP, and FortiAnalyzer logging has been enabled in the Security Fabric settings.



## To enable FortiAnalyzer as a Fabric SP in the GUI:

1. In FortiAnalyzer, go to *System Settings > Admin > SAML SSO*.
2. For *Single Sign-On Mode*, click *Fabric SP* and enter the *SP Address*.

**System Settings** ▾ admin ▾

**SAML SSO**

**Single Sign-On Mode** Disabled Identity Provider (IdP) Service Provider (SP) **Fabric SP**

In Fabric mode, an SSO administrator is created for each Security Fabric. When a user logs in via Fabric SSO, the Fabric IdP provides the user's profile name. If this system has a profile with the matching name, the profile is assigned to the user. Otherwise, the profile of the SSO administrator is assigned to the user by default.

SP Address:

Default Admin Profile: Restricted\_User ▾

**Fabric IdPs**

Delete Column Settings ▾ Search

Root Device	ADOM Name	Status	IdP Settings
No record found. You may configure Fabric IdPs by initiating a connection from your Fabric root device.			

Apply

3. Click *Apply*.

FortiAnalyzer will automatically register itself on the FortiGate as an appliance visible in the list of SPs. Go to *Security Fabric > Fabric Connectors*, edit the *Security Fabric Setup* connector, then click *Advanced Options* to view the list of SPs.

**SAML SSO** ×

Mode: Disable **Identity Provider (IdP)** Service Provider (SP)

IdP address:  Use Current Browser Address

IdP certificate: Fortinet\_Factory ▾ Download

**Service Providers**

+ Create New Edit Delete Search

Name	Prefix	FortiGate
csf_robot.csf:4432	csf_lom9dgyvOy995017i7zm70yknxa9cm5	FGTB-1
csf_172.17.48.225:4434	csf_7mt1h4mShtjIn1rcwa8ejl6xxg51mlk	FGTD
csf_robot.csf:4433	csf_0xj7kdjfl7avereh7shw4xkr4fzwrp	FGTC
appliance_172.17.48.225:4253	csf_p0m9dvltwt28r3gt87runs2nb929mwz	

OK Cancel

## To enable FortiAnalyzer as a Fabric SP in the CLI:

1. In FortiAnalyzer, enable the device as a Fabric SP:

```
config system saml
    set status enable
    set role FAB-SP
    set server-address "172.17.48.225:4253"
end
```

FortiAnalyzer will register itself on the FortiGate as an appliance. To view the configuration in FortiOS:

```
show system saml
config service-providers
    edit "appliance_172.17.48.225:4253"
        set prefix "csf_p0m9dvltwt28r3gt87runs2nb929mwz"
        set sp-entity-id "http://172.17.48.225:4253/metadata/"
        set sp-single-sign-on-url "https://172.17.48.225:4253/saml/?acs"
        set sp-single-logout-url "https://172.17.48.225:4253/saml/?sls"
        set sp-portal-url "https://172.17.48.225:4253/saml/login/"
```

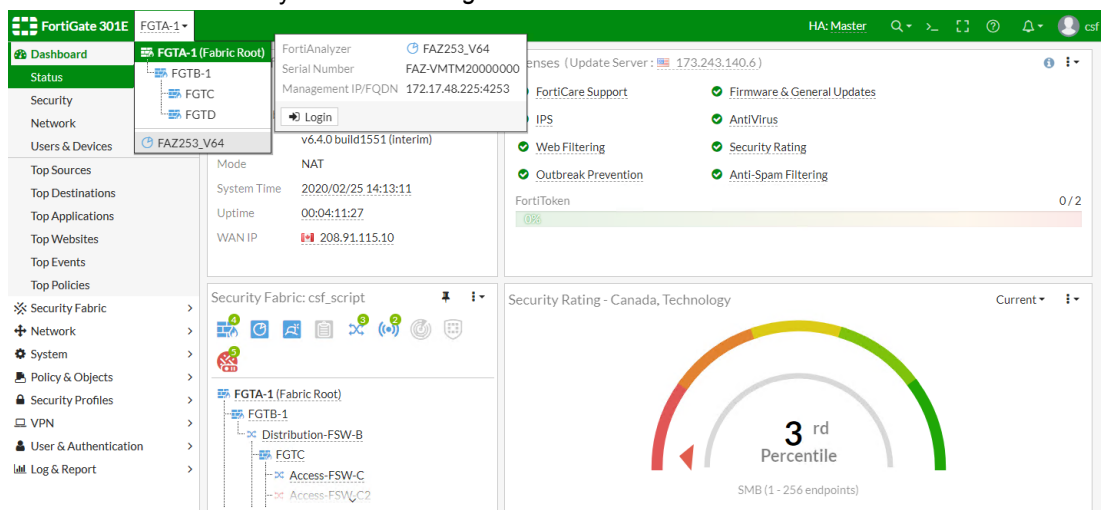
```

config assertion-attributes
    edit "username"
    next
    edit "profilename"
        set type profile-name
    next
end
next
end

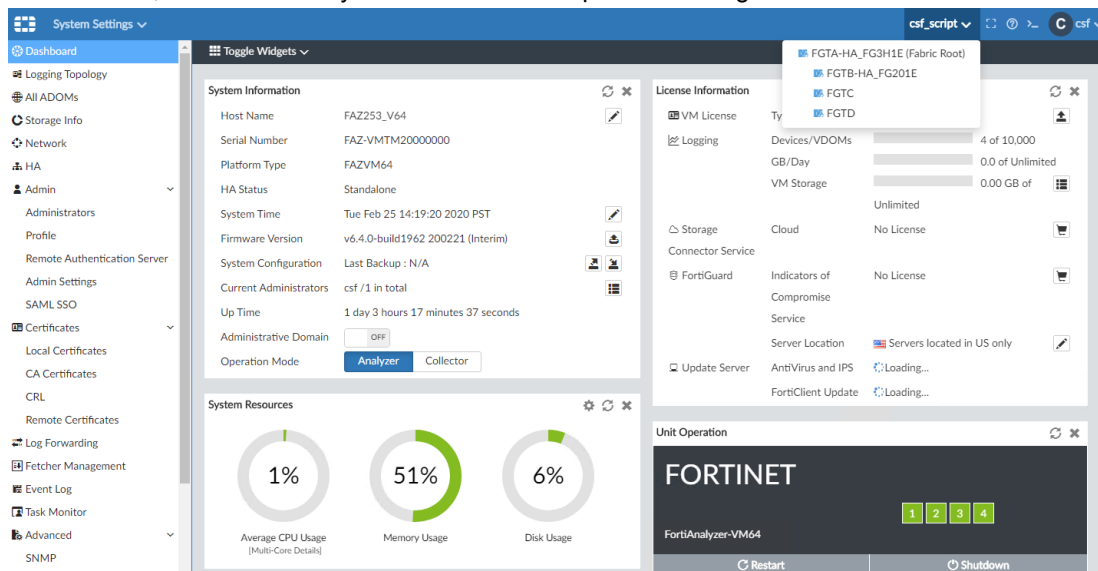
```

### To navigate between devices using SAML SSO:

1. Log in to the root FortiGate.
2. In the toolbar, click the device name to display the Security Fabric members dropdown.
3. Hover over the FortiAnalyzer and click *Login*.



4. Log in to the FortiAnalyzer using SAML SSO.
5. In the toolbar, click the Security Fabric members dropdown to navigate between other FortiGates.



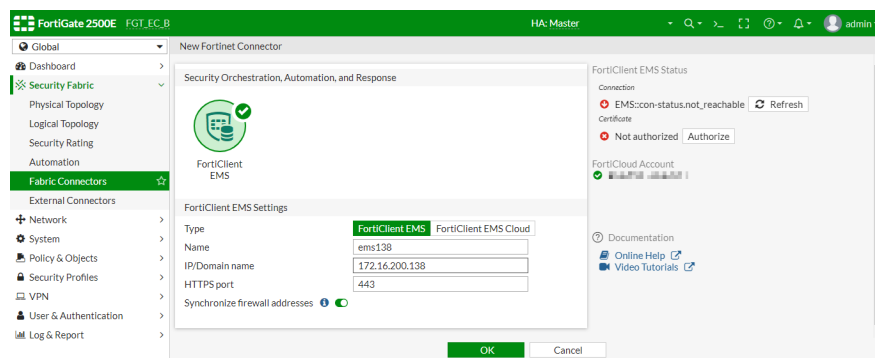
## Simplify FortiClient EMS setup

EMS configurations are now centralized under one configuration card on the *Fabric Connectors* page. Certificates are the main mode of authentication and authorization. The certificate validity is verified against the issuer CA, and then presented to the user to authorize. A certificate attribute has been added to `endpoint-control fctems`, and EMS certificates can be verified with `execute fctems verify`.

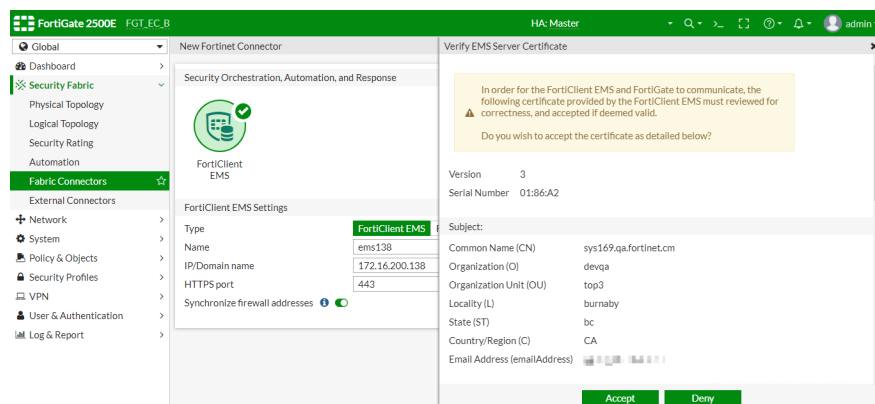
The following examples presume the EMS certificate has already been configured.

### To configure an on-premise FortiClient EMS server to the Security Fabric in the GUI:

1. On the root FortiGate, go to *Security Fabric > Fabric Connectors*.
2. Click *Create New* and click *FortiClient EMS*.
3. For *Type*, click *FortiClient EMS*.
4. Enter a name and IP address.
5. Click *OK*.

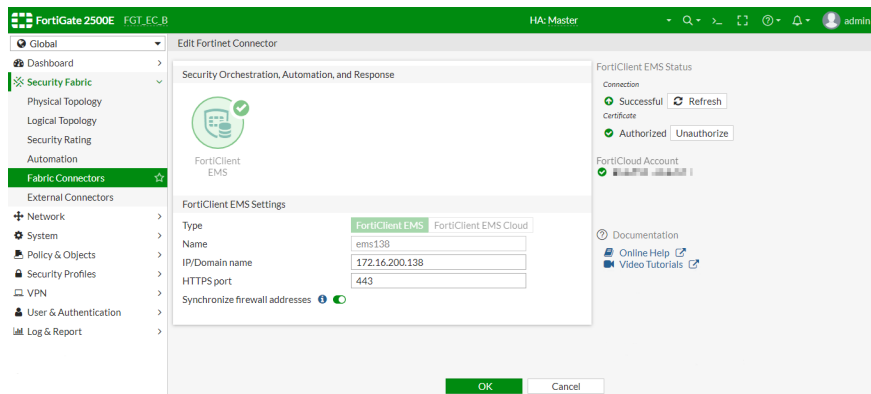


A window appears to verify the EMS server certificate:



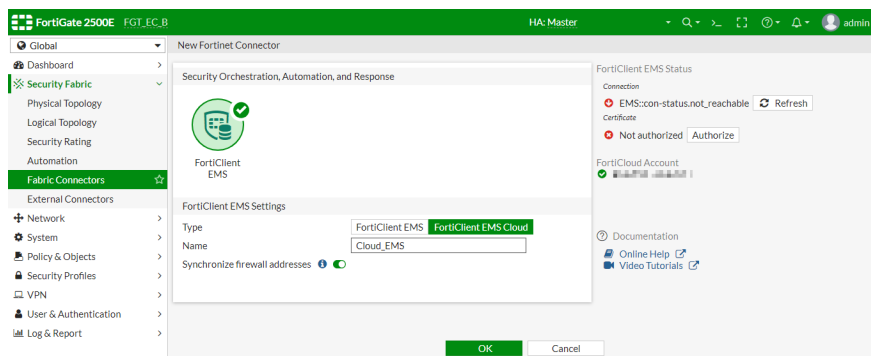
6. Click *Accept*.

The *FortiClient EMS Status* section displays a *Successful* connection and an *Authorized* certificate:



### To configure a FortiClient EMS Cloud server to the Security Fabric in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New* and click *FortiClient EMS*.
3. For *Type*, click *FortiClient EMS Cloud*.
4. Enter a name.
5. Click *OK*.



A window appears to verify the EMS server certificate.

6. Click *Accept*.
- The *FortiClient EMS Status* section displays a *Successful* connection and an *Authorized* certificate.

### To configure an on-premise FortiClient EMS server to the Security Fabric in the CLI:

```
config endpoint-control fctems
  edit "ems138"
    set server "172.16.200.138"
    set certificate "REMOTE_Cert_1"
  next
end
```

### To configure a FortiClient EMS Cloud server to the Security Fabric in the CLI:

```
config endpoint-control fctems
  edit "Cloud_EMS"
    set fortinetone-cloud-authentication enable
    set certificate "REMOTE_Cert_1"
```

```
next
end
```

**To verify an EMS certificate in the CLI:**

```
# execute fctems verify ems137
```

```
Subject:      C = CA, ST = bc, L = burnaby, O = devqa, OU = top3, CN =
sys169.qa.fortinet.cm, emailAddress = xxxx@xxxxxxxx.xxx
Issuer:       CN = 155-sub1.fortinet.com
Valid from:   2017-12-05 00:37:57 GMT
Valid to:     2027-12-02 18:08:13 GMT
Fingerprint: D3:7A:1B:84:CC:B7:5C:F0:A5:73:3D:BB:ED:21:F2:E0
Root CA:      No
Version:      3
Serial Num:
01:86:a2
Extensions:
  Name:       X509v3 Basic Constraints
  Critical:   yes
  Content:
  CA:FALSE

  Name:       X509v3 Subject Key Identifier
  Critical:   no
  Content:
  35:B0:E2:62:AF:9A:7A:E6:A6:8E:AD:CB:A4:CF:4D:7A:DE:27:39:A4

  Name:       X509v3 Authority Key Identifier
  Critical:   no
  Content:
  keyid:66:54:0F:78:78:91:F2:E4:08:BB:80:2C:F6:BC:01:8E:3F:47:43:B1

DirName:/C=CA/ST=bc/L=burnaby/O=devqa/OU=top3/CN=fac155.fortinet.com/emailAddress=xyguo@fort
inet.com
serial:01:86:A4

  Name:       X509v3 Subject Alternative Name
  Critical:   no
  Content:
  DNS:sys169.qa.fortinet.cm

  Name:       X509v3 Key Usage
  Critical:   no
  Content:
  Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key
Agreement, Certificate Sign, CRL Sign, Encipher Only, Decipher Only

  Name:       X509v3 Extended Key Usage
  Critical:   no
  Content:
  TLS Web Server Authentication, TLS Web Client Authentication
```

```
EMS configuration needs user to confirm server certificate.
Do you wish to add the above certificate to trusted remote certificates? (y/n)y
```

## Simplify the synchronization of EMS tags and configurations

A new option under the FortiClient EMS settings consolidates the setup of EMS connectors to support EMS tags. EMS tags are pulled and automatically synced with the EMS server. They are converted into read-only dynamic firewall addresses that can be used in firewall policies, routing, and so on.

These examples presume the following have been configured in FortiClient EMS:

- Tags have been created on the *Compliance Verification > Compliance Verification Rules* page.

The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar has a menu with options like Dashboard, Endpoints, Quarantine Management, Software Inventory, Endpoint Policy, Endpoint Profiles, Manage Installers, Policy Components, Telemetry Server Lists, Compliance Verification, Host Tag Monitor, Fabric Device Monitor, Administration, and System Settings. The 'Compliance Verification' section is expanded, showing 'Compliance Verification Rules'. The main table lists the following rules:

Name	Tag	Enabled	Comments
ems137_file_tag	ems137_file_tag	✓	
ems137_macos_tag	ems137_macos_tag	✓	
ems137_vuln_critical_tag	ems137_vuln_critical_tag	✓	
ems137_win10_tag	ems137_win10_tag	✓	
ems137_winscp_tag	ems137_winscp_tag	✓	

- There are registered users who match the defined tags that are visible on the *Compliance Verification > Host Tag Monitor* page.

The screenshot shows the FortiClient Endpoint Management Server interface with the 'Host Tag Monitor' section selected. It displays a table of endpoints categorized by tag.

Endpoint	User	OS	IP	Tagged on
<b>ems137_vuln_critical_tag (3)</b>				
DESKTOP-FJEVH8U	frank	Microsoft Windows 10 Professional Edition, 64-bit...	10.1.100.120	2020-03-15 12:59:28
frank-PC	tester1	Microsoft Windows 7 Professional Edition, 32-bit...	10.1.100.198	2020-03-15 15:07:54
VAN-200492-PC	qa	Microsoft Windows 10 Professional Edition, 64-bit...	192.168.1.110	2020-03-16 13:39:40
<b>ems137_win10_tag (2)</b>				
DESKTOP-FJEVH8U	frank	Microsoft Windows 10 Professional Edition, 64-bit...	10.1.100.120	2020-03-15 12:59:28
VAN-200492-PC	qa	Microsoft Windows 10 Professional Edition, 64-bit...	192.168.1.110	2020-03-16 13:39:40
<b>ems137_winscp_tag (1)</b>				
LHWin7A	Administrator	Microsoft Windows 7 Enterprise Edition, 32-bit Se...	100.100.100.141	2020-03-16 10:57:31

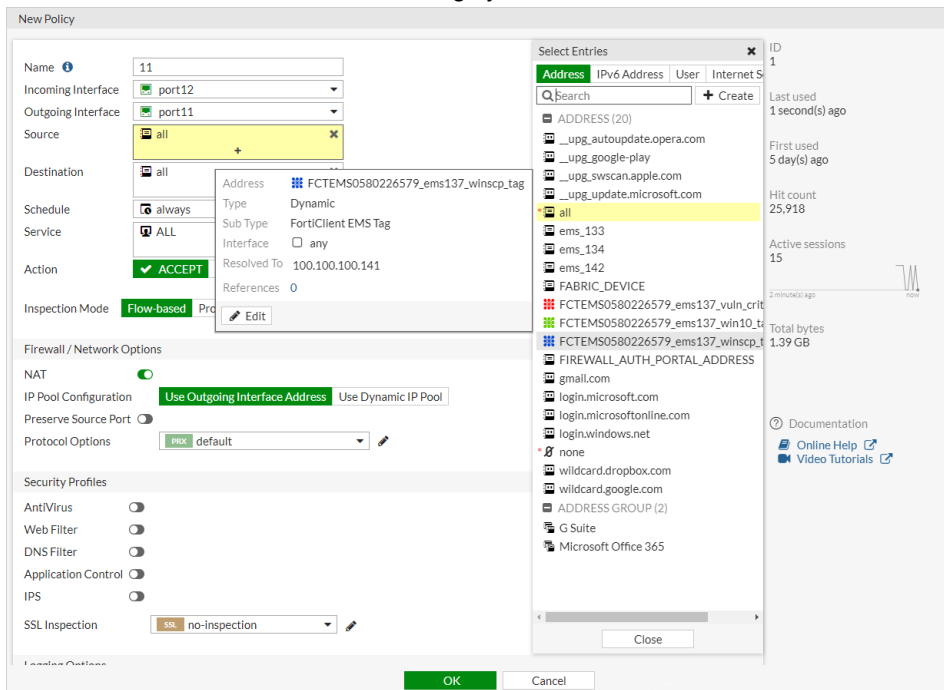
### To configure FortiClient EMS with tag synchronization in the GUI:

- Configure the EMS Fabric Connector:
  - On the root FortiGate, go to *Security Fabric > Fabric Connectors*.
  - Click *Create New* and click *FortiClient EMS*.
  - Enable *Synchronize firewall addresses*.

The screenshot shows the 'FortiClient EMS Settings' configuration page. It includes a status icon with a green checkmark and the text 'FortiClient EMS'. Below, the settings are as follows:

Type	FortiClient EMS
Name	ems137
IP/Domain name	172.16.200.137
HTTPS port	
Synchronize firewall addresses	<input checked="" type="checkbox"/> Automatically create and synchronize firewall address for all EMS tags

- d. Configure the other settings as needed and validate the certificate.
- e. Click OK.
2. Go to *Policy & Objects > Addresses* and hover over the EMS tag to view which IPs it resolves to.
3. Configure a firewall policy:
  - a. Go to *Policy & Objects > Firewall Policy* and create a new policy.
  - b. For the *Source Address*, add the EMS tag dynamic address.



- c. Configure the other settings as needed.
- d. Click OK.

## To configure FortiClient EMS with tag synchronization in the CLI:

1. Configure the EMS Fabric Connector:

```
config endpoint-control fctems
edit "ems137"
    set fortinetone-cloud-authentication disable
    set server "172.16.200.137"
    set https-port 443
    set source-ip 0.0.0.0
    set pull-sysinfo enable
    set pull-vulnerabilities enable
    set pull-avatars enable
    set pull-tags enable
    set call-timeout 5000
    set certificate "REMOTE_Cert_1"
next
end
```

2. Verify which IPs the dynamic firewall address resolves to:

```
# diagnose firewall dynamic list
List all dynamic addresses:
```

```

FCTEMS0580226579_ems137_vuln_critical_tag: ID(118)
  ADDR(10.1.100.120)
  ADDR(10.1.100.198)

FCTEMS0580226579_ems137_winscp_tag: ID(155)
  ADDR(100.100.100.141)

FCTEMS0580226579_ems137_win10_tag: ID(182)
  ADDR(10.1.100.120)

# diagnose firewall dynamic address FCTEMS0580226579_ems137_vuln_critical_tag
FCTEMS0580226579_ems137_vuln_critical_tag: ID(118)
  ADDR(10.1.100.120)
  ADDR(10.1.100.198)

Total dynamic list entries: 1.
Total dynamic addresses: 2
Total dynamic ranges: 0

```

3. Configure a firewall policy that uses the EMS tag dynamic firewall address as a source.

## Allow FortiNAC to join the Security Fabric

A FortiNAC device can be added to the Security Fabric on the root FortiGate. After the device has been added and authorized, you can log in to the FortiNAC from the FortiGate topology views.



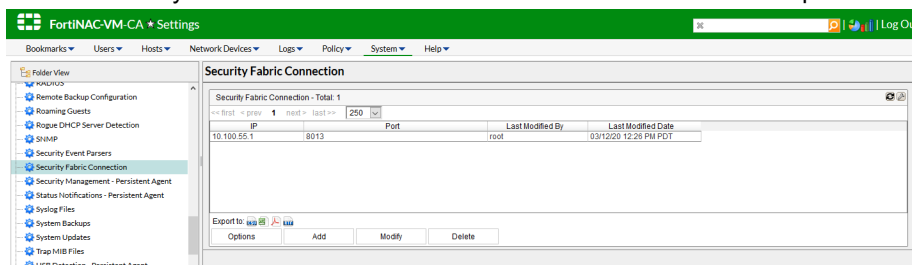
Adding a FortiNAC to the Security Fabric requires a FortiNAC with a license issued in the year 2020 that includes an additional certificate. The device cannot be added if it has an older license. Use the `licensetool` in the FortiNAC CLI to determine if your license includes the additional certificate

### To add a FortiNAC to the Security Fabric:

1. On the FortiNAC, configure telemetry and input the IP address of the root FortiGate.
2. On the root FortiGate, authorize the FortiNAC.
3. Verify the connection status in the topology views.

### To configure the FortiNAC:

1. Go to *System > Settings*, and in the *Folder View* select *Security Fabric Connection*.
2. Add a new entry with the root FortiGate device's IP address. The default port is 8013.

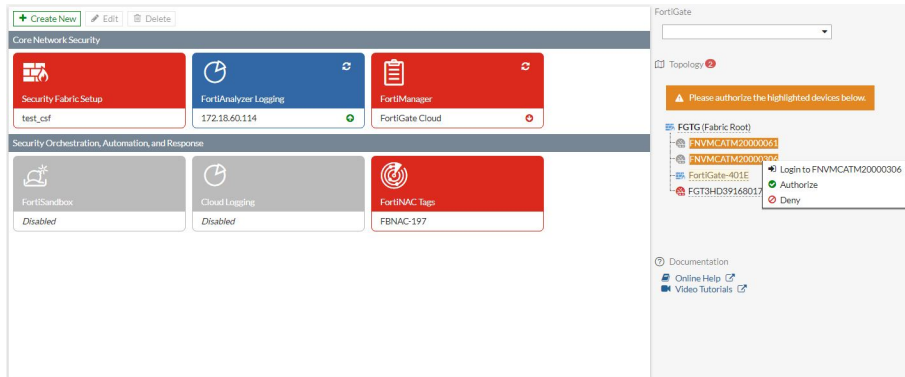


See [Security Fabric Connection](#) in the *FortiNAC Administration Guide* for more information.



### To authorize the FortiNAC on the root FortiGate in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. The FortiNAC device will be highlighted in the topology list in the right panel with the status *Waiting for Authorization*.
3. Click on the highlighted FortiNAC and select *Authorize*.



Optionally, you can also deny authorization to the FortiNAC to remove it from the list.



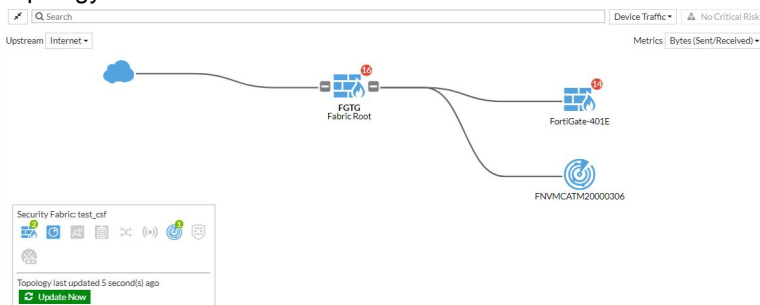
Joining a FortiNAC to the Security Fabric is not related to FortiNAC Tags FSSO connectors. See [FortiNAC endpoint connector](#) for information about the FSSO connector.

### To authorize the FortiNAC on the root FortiGate in the CLI:

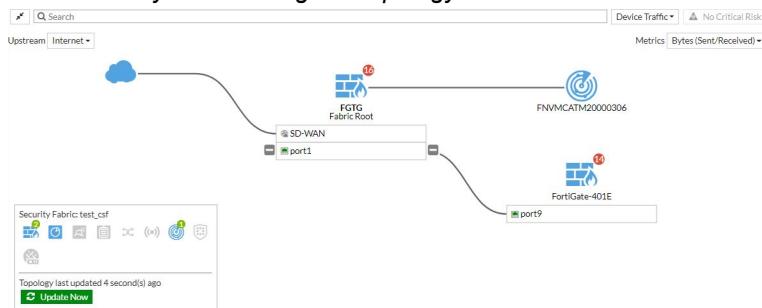
```
config system csf
  config trusted-list
    edit "FNVMCATM20000306"
      set action accept
    next
  end
end
```

### To verify the connection status:

1. After the FortiNAC is authorized, go to *Security Fabric > Physical Topology* and confirm that it is included in the topology.



2. Go to *Security Fabric > Logical Topology* and confirm the FortiNAC is also displayed there.

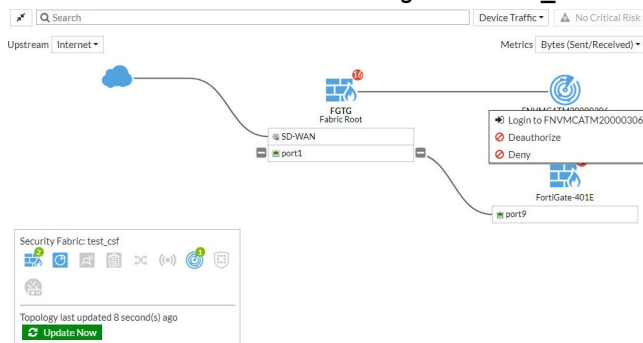


3. Run the following command in the CLI to view information about the FortiNAC device's status:

```
# diagnose sys csf downstream-devices fortinac
{
  "path": "FG5H1E5818900126:FNVMCATM20000306",
  "mgmt_ip_str": "10.1.100.197",
  "mgmt_port": 0,
  "admin_port": 8443,
  "serial": "FNVMCATM20000306",
  "host_name": "adnac",
  "device_type": "fortinac",
  "upstream_intf": "port2",
  "upstream_serial": "FG5H1E5818900126",
  "is_discovered": true,
  "ip_str": "10.1.100.197",
  "downstream_intf": "eth0",
  "authorizer": "FG5H1E5818900126",
  "idx": 1
}
```

### To log in to the FortiNAC from the FortiGate:

1. On the FortiGate, go to *Security Fabric > Physical Topology* or *Security Fabric > Logical Topology*.
2. Click on the FortiNAC and select *Login to <serial\_number>*.



A new tab will open to the FortiNAC log in page.

3. Enter the username and password to log in to the FortiNAC.

## Redesign Fortinet Fabric Connectors and Fabric setup pages

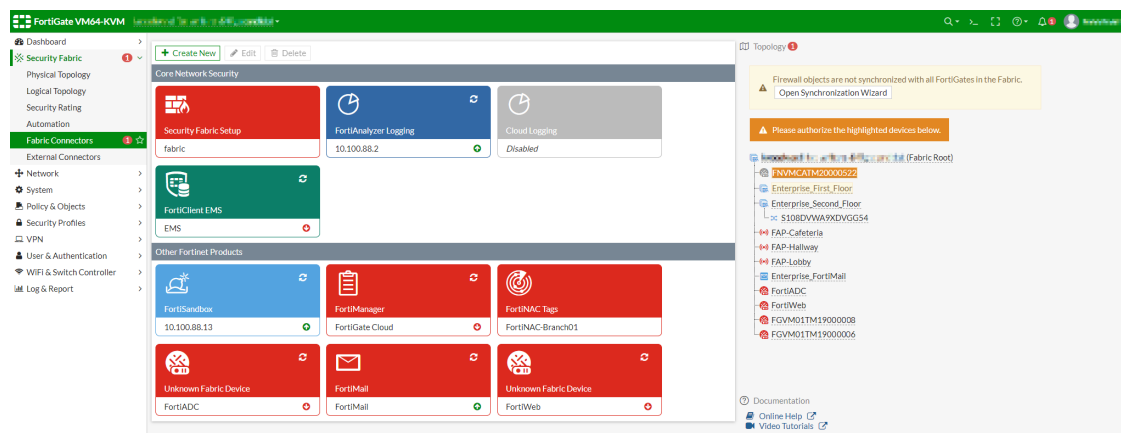
In FortiOS 6.4.0 there have been several changes to simplify the GUI for the Security Fabric menu.

- The *Security Fabric Settings* page has been renamed to *Fabric Connectors* and all the settings under it now show up as separate cards. The cards that appear by default are: *Security Fabric Setup*, *FortiAnalyzer Logging*, *FortiManager*, *FortiSandbox*, and *Cloud Logging*.
- The new *Fabric Connectors* menu contains a card view similar to *External Connectors* for various Fortinet products (FortiSandbox, FortiManager, Cloud Logging, and so on).
- The *Fabric Connectors* menu has been renamed to *External Connectors* where third-party connectors are configured.
- Each card has a separate page with its own edit dialog view.
- The topology tree, various statistics, and connectivity results have been moved from the main dialog to the gutter.

## Fabric Connectors page

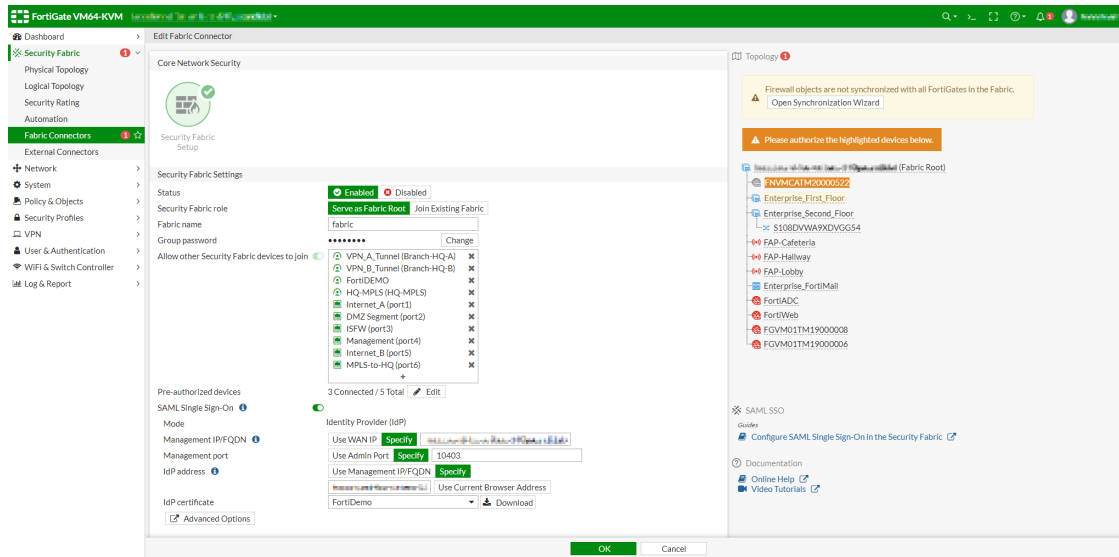
This page displays all configured Security Fabric Devices with their own card. The card also display the device connectivity status with a green up arrow or a red down arrow.

The topology tree and notifications are displayed in the gutter. In this example, there is a device that requires authorization.



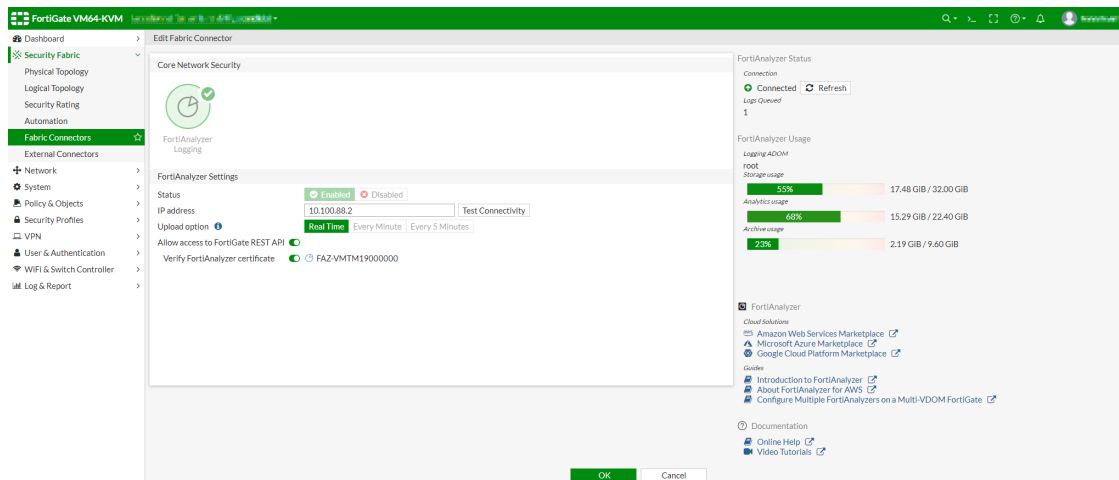
## Security Fabric Setup page

This page displays the Security Fabric settings, including SAML SSO. In previous versions these settings were under the *FortiTelemetry* section. The topology tree is also displayed in the gutter.



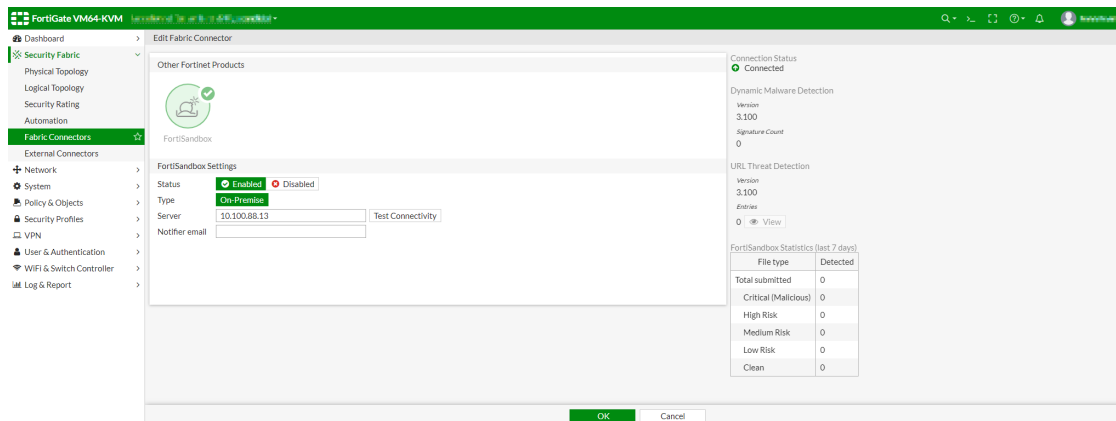
## FortiAnalyzer Logging page

The gutter in this page displays the connection status and usage information.



## FortiSandbox page

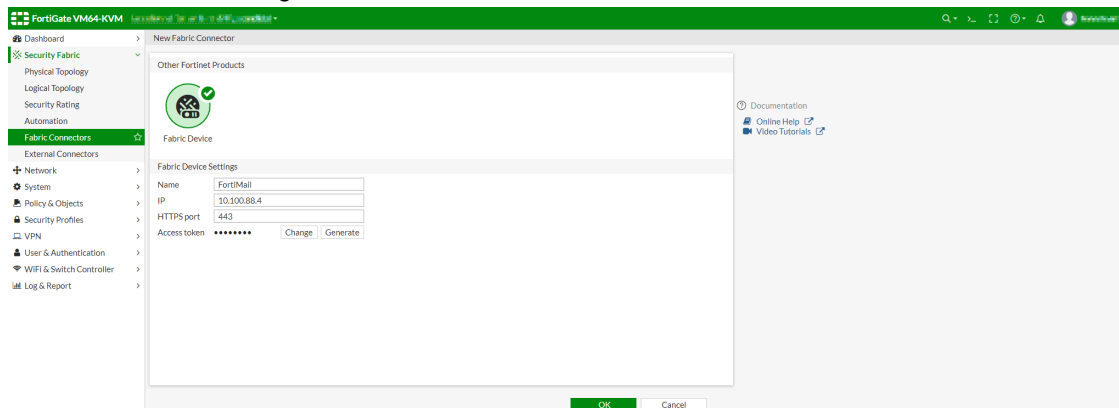
The gutter in this page displays the connection status, dynamic malware and URL threat detection information, and FortiSandbox statistics.



## Adding a new Fabric connector

### To configure a FortiMail connector:

1. Go to *Security Fabric > Fabric Connectors* and click *Create New*.
2. Click *Fabric Device*.
3. Enter the FortiMail settings as needed.



4. Click *OK*.

The FortiGate will attempt to connect to the device to authorize it. Once the device is authorized, the device name will no longer be displayed as *Unknown Fabric Device* in the card. The corresponding device name and icon are displayed in the card.

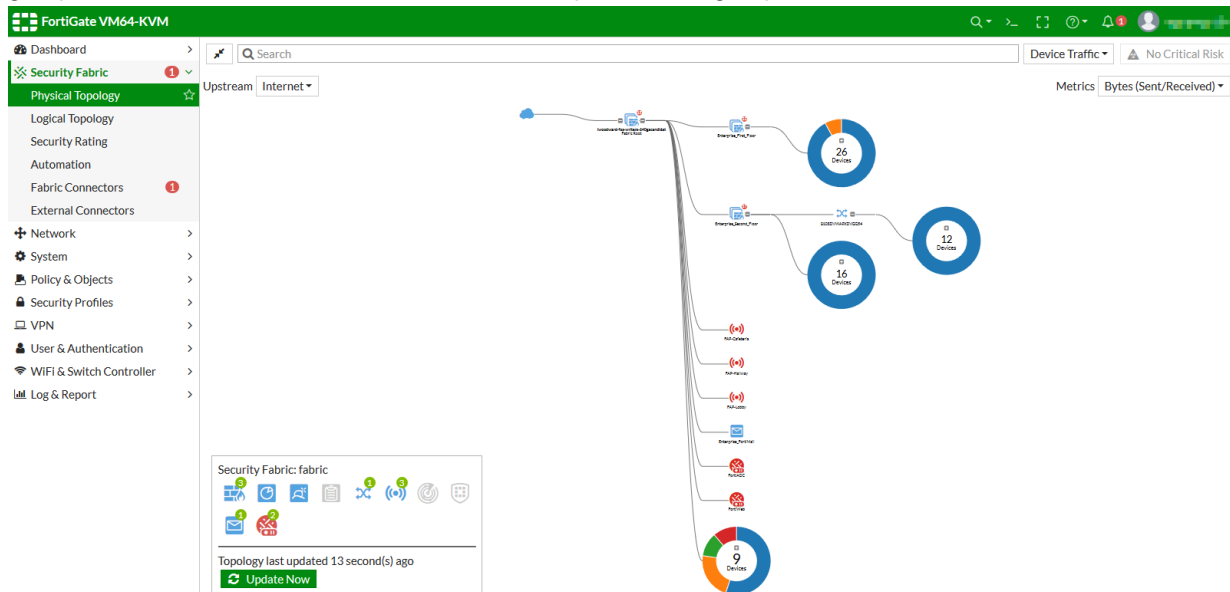


## Display endpoints in Topology using donut chart

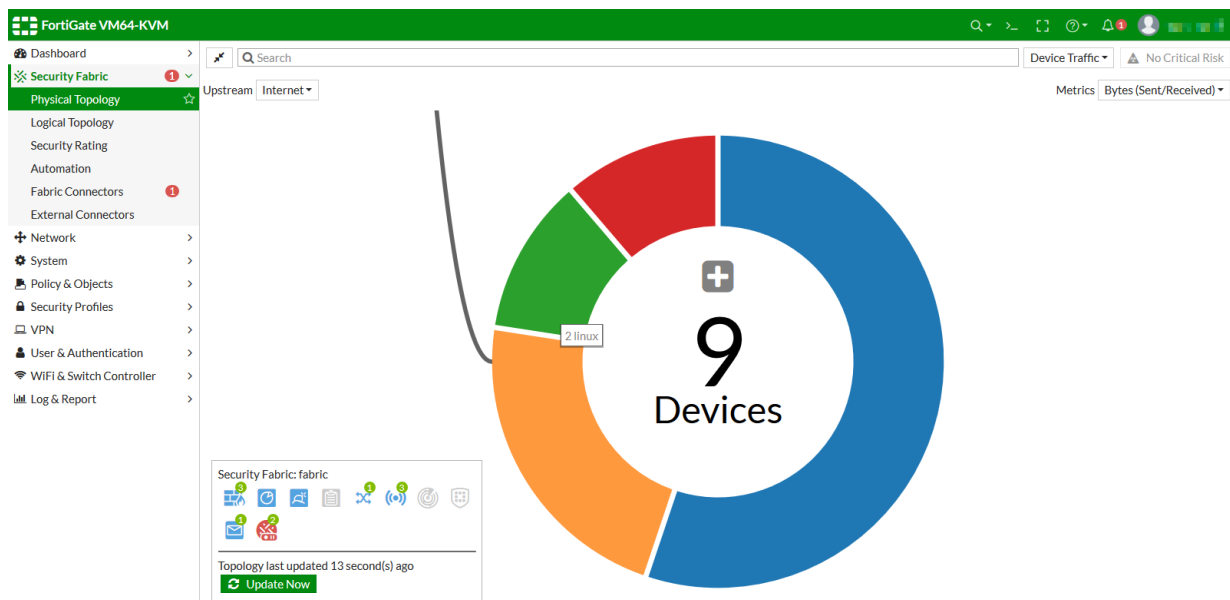
On the Physical and Logical Topology pages, the Device Traffic and Device Count views now display endpoint groups as donut charts. Each sector of the donut chart represents a different endpoint operating system. This new donut chart display allows for faster loading times and provides more stability with zoom operations. This improvement is especially useful for deployments with a large number of endpoints, while retaining the bubble pack endpoint view from earlier versions of FortiOS.

## To view endpoints in Topology using donut charts:

1. Go to *Security Fabric > Physical Topology* or *Logical Topology*.
2. From the *Endpoint Option* dropdown list, select *Device Traffic* or *Device Count*. FortiOS represents each endpoint group as a donut chart, with the total number of endpoints in the group in the center of the chart.



To zoom in on a donut chart, click any chart sector. Each sector represents a different endpoint OS. Hovering over each sector allows you to see the OS that the sector represents and the number of endpoints that have that OS installed.

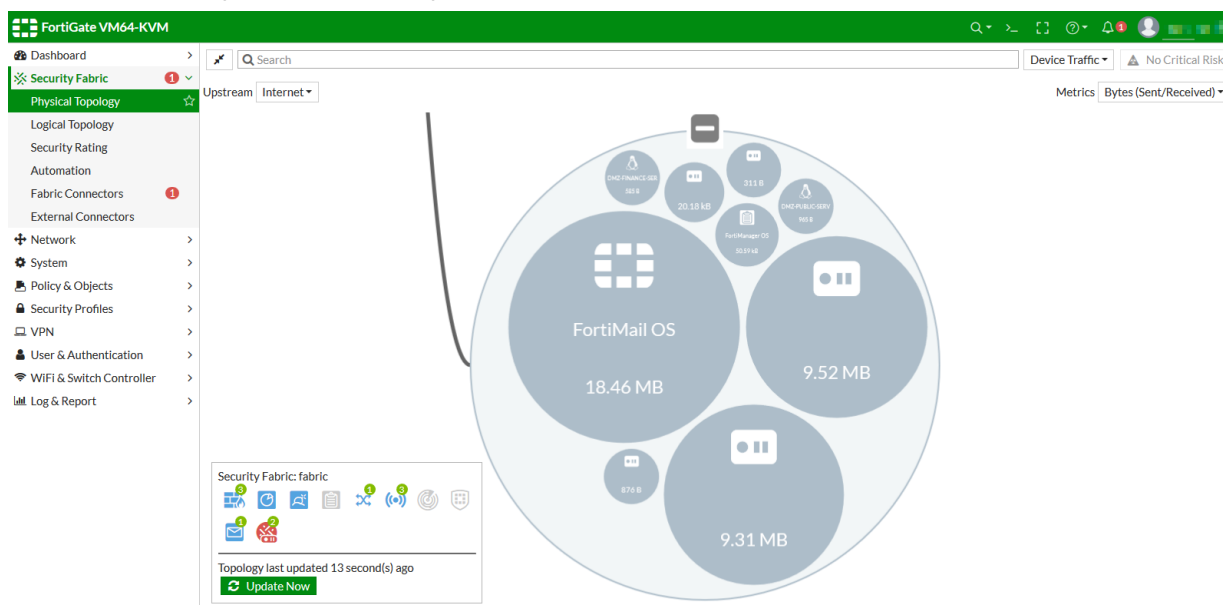


In this example, the endpoint group contains a total of nine endpoints, with the following OSes installed:

Donut sector color	OS	Number of endpoints
Orange	Linux	2

Donut sector color	OS	Number of endpoints
Green	FortiMail	1
Red	FortiManager	1
Blue	Other	5

To view the endpoint group in a bubble pack display, click the + button in the center of the donut chart. You can view each individual endpoint in the bubble pack view.



To return to the donut chart display, click the - button at the top of the bubble.

## Using the root FortiGate with disk to store historic user and device information

This backend implementation allows the root FortiGate in a Security Fabric to store historic user and device information in a database on its disk. This will allow administrators to visualize users and devices over a period of time.

A new daemon, `user_info_history`, stores this data on the disk. The information source for the historical data will be the `user_info` daemon, which would be recorded on the disk when `user_info` notifies `user_info_history` that a user has logged out or the device is no longer connected.

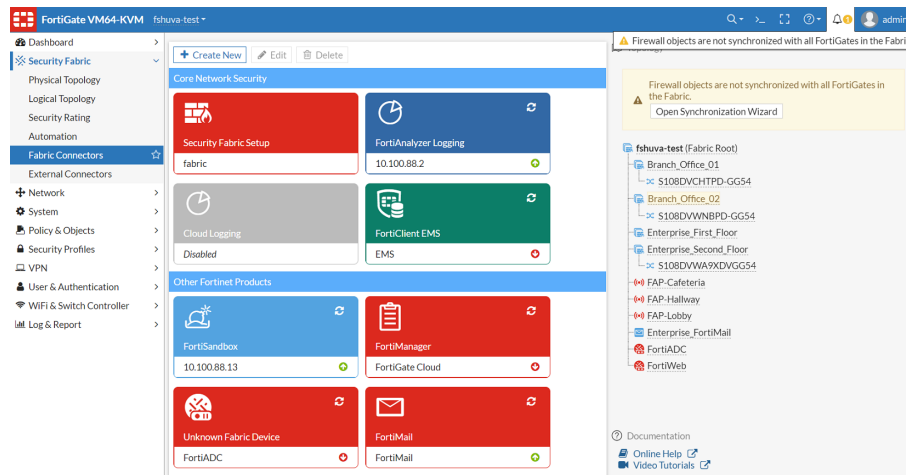
## Synchronizing objects across the Security Fabric

When the Security Fabric is enabled, various objects such as addresses, services, and schedules are synced from the upstream FortiGate to all downstream devices by default. The firewall object synchronization wizard helps identify objects that are out of sync and resolves any conflicts. Objects that are out of sync are highlighted in yellow in the GUI.



Further updates were made to synchronization in FortiOS 6.4.4. See [Improvements to synchronizing objects across the Security Fabric 6.4.4 on page 62](#) for more information.

In this example, the notifications icon displays a message that *Firewall objects are not synchronized with all the FortiGates in the Fabric*. In the topology tree, *Branch\_Office\_02* is highlighted in yellow because it is out of sync.

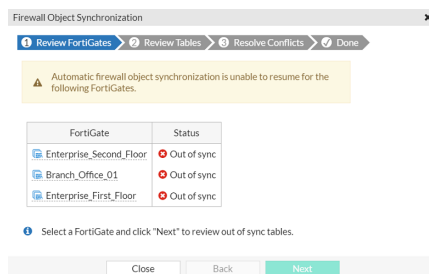


In this example, the tooltip displays a caution icon that the device is out of sync.

FortiGate	Branch_Office_01
Hostname	Branch_Office_01
Serial Number	FGVM01TM19000000
HA Mode	stand-alone
Model	FortiGate VM64-KVM
Version	v6.4.0 build1579
Operation Mode	NAT
Management IP/FQDN	fshuva-test.fortidemo.fortinet.com This FortiGate connects to upstream FortiGate via a VPN
Management Port	10423
Object Sync Status	Out of sync
Topology	fshuva-test Branch_Office_01 1 Downstream Fabric Devices
CPU Usage	54%
Memory Usage	54%
Session Count	645

## To use the firewall object synchronization wizard in the GUI:

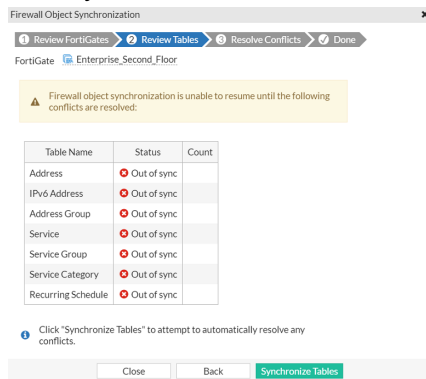
1. Go to *Security Fabric > Fabric Connectors* and click *Open Synchronization Wizard*.  
A list of FortiGates and their synchronization status displays.



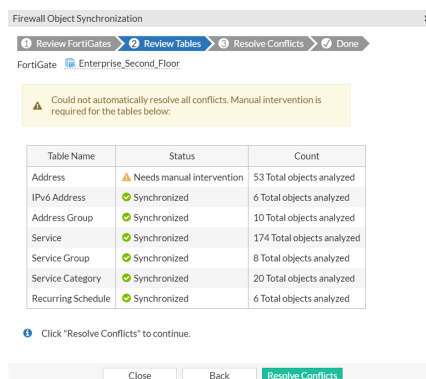
2. Select a FortiGate that is *Out of sync* and click *Next*.  
A list of tables and their synchronization status displays.



### 3. Click *Synchronize Tables*.



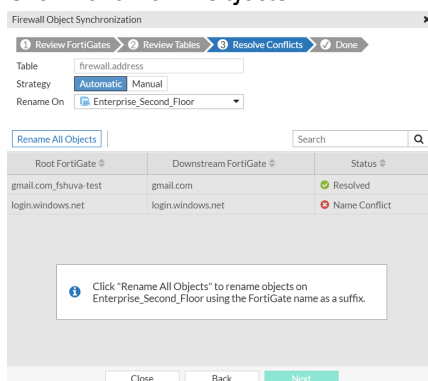
The FortiGate attempts to automatically resolve the conflicts. In this example, the address table requires manual intervention.



### 4. Click *Resolve Conflicts*.

### 5. For *Strategy*, choose one of the following.

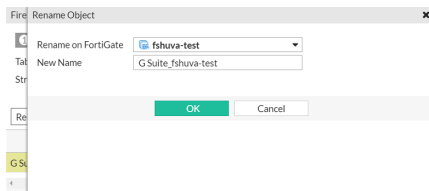
- Automatic resolve (automatically resolves all the name conflicts and renames them on the selected FortiGate using the FortiGate name as a suffix):
  - Click *Automatic*.
  - Click *Rename All Objects*.



### b. Manual resolve:

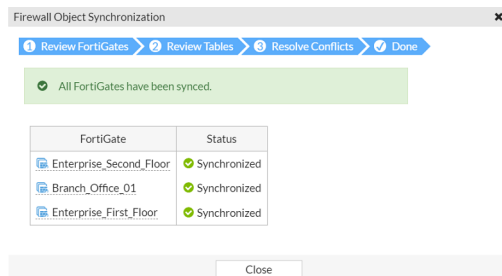
- Click *Manual*.
- Double-click an object and re-name it.

## iii. Click OK.



## 6. Click Next.

An updated list of FortiGates and their synchronization status displays.



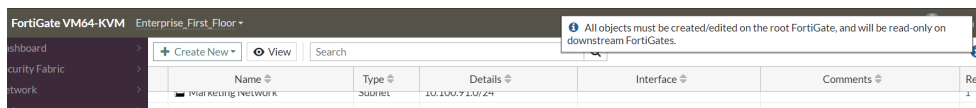
## 7. Click Close.

## To verify object synchronization on downstream devices:

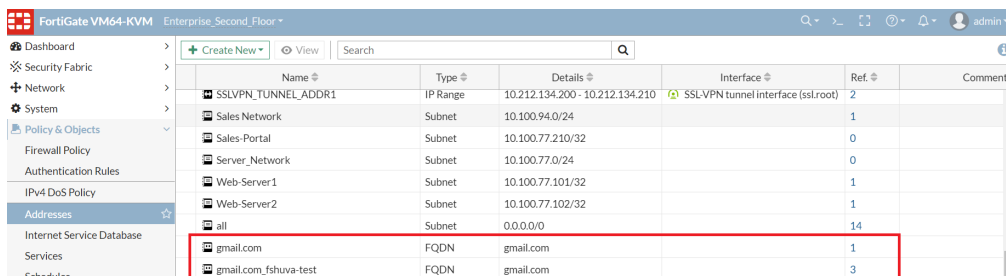
## 1. Log in to a downstream device.

2. Go to *Policy & Objects > Addresses*.

- An information bubble displays the following: *All objects must be created/edited on the root FortiGate, and will be read-only on downstream FortiGates.*



- The following example shows an object that exists on both upstream (Enterprise\_Second\_Floor) and downstream (fshuva-test) FortiGates. On the downstream device, there is an existing *gmail.com*, and another object, *gmail.com\_fshuva-test*, that was resolved by adding the suffix of the upstream FortiGate name to the end.



- In this example, an object created on the upstream FortiGate is synchronized to a downstream FortiGate.

Name	Type	Details	Interface	Comments	Ref.
Sales-Portal	Subnet	10.100.77.210/32			1
Server_Network	Subnet	10.100.77.0/24			1
This_is_created_on_the_root_device	Subnet	0.0.0.0/0		This object was created on the root device	0
Web-Server1	Subnet	10.100.77.101/32			1
Web-Server2	Subnet	10.100.77.102/32			1
all	Subnet	0.0.0.0/0			19
gmail.com	FQDN	gmail.com			0

The same object appears automatically on the downstream device.

Name	Type	Details	Interface	Comments	Ref.
Marketing-DB	Subnet	10.100.77.230/32			0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.2...	SSL-VPN tunnel interface (ssl.root)		2
Sales-Network	Subnet	10.100.94.0/24			1
Sales-Portal	Subnet	10.100.77.210/32			0
Server_Network	Subnet	10.100.77.0/24			0
This_is_created_on_the_root_device	Subnet	0.0.0.0/0		This object was created on the root device	0
Web-Server1	Subnet	10.100.77.101/32			1

## CLI commands

Object synchronization can be configured with the following commands:

```
config system csf
    set fabric-object-unification [default | local]
    set configuration-sync [default | local]
    ...
next
end
```

Parameter	Description
fabric-object-unification	<i>default:</i> Global CMDB objects will be synchronized in Security Fabric. <i>local:</i> Global CMDB objects will not be synchronized to and from this device.
configuration-sync	<i>default:</i> Synchronize configuration for FortiAnalyzer, FortiSandbox, and Central Management to root node. <i>local:</i> Do not synchronize configuration with root node.

## Streamlined Fortinet Security Fabric setup between FortiGates - 6.4.2

When you log in to an unauthorized, downstream FortiGate device, the log in prompt includes the option to authorize the device on the root FortiGate device.

When the Security Fabric is disabled on the FortiGate, and a neighboring FortiGate is detected on the same network using LLDP, the log in prompt gives the option to join the Security Fabric.

A downstream FortiGate device's authorization status can also be reviewed from Fabric Connectors gutter page.

## To authorize a downstream FortiGate:

1. Log in to the unauthorized, downstream device.

2. On the *Fabric Setup* step, click *Review authorization on root FortiGate*. A pop-up window opens to a log in screen for the root FortiGate.

3. Enter the log in credentials for the root FortiGate, then click *Login*. A list of pending authorizations is shown.

4. Select *Allow* and then click *OK* to authorize the downstream FortiGate. You can also select *Deny* to reject the authorization, or *Later* to postpone the decision to the next time that you log in. When authorization is allowed, the pop-up window closes, and the log in prompt shows that the downstream FortiGate has been authorized.

Setup Progress	Fabric Setup
Specify Hostname ✓	<div>⚠ Connect this FortiGate to the detected Security Fabric via an upstream FortiGate.</div> <div>Upstream FortiGate 10.100.88.1 (FGT-Root)</div> <div>Join Existing Fabric <input checked="" type="checkbox"/> Successfully authorized by root FortiGate.</div> <div>Review Fabric Settings Done</div>
Register with FortiCare ✓	
Change Your Password ✓	
Dashboard Setup ✓	
> Fabric Setup ✓	

- Click *Done* to log in to the downstream FortiGate.

### To join an existing fabric that is detected on the same network:

- Log in to the device.

Setup Progress	Fabric Setup
Specify Hostname ✓	<div>⚠ Connect this FortiGate to the detected Security Fabric via an upstream FortiGate.</div> <div>Upstream FortiGate 192.168.111.99</div> <div>Join Existing Fabric <input type="checkbox"/></div> <div>Previous Later</div>
Register with FortiCare	
Change Your Password ✓	
Upgrade Firmware	
Dashboard Setup ✓	
> Fabric Setup	

- On the *Fabric Setup* step, enable *Join Existing Fabric*.
- Authorize the FortiGate, as previously shown.

### To review authorization on the downstream FortiGate:

- Go to *Security Fabric > Fabric Connectors*.
- In the gutter on the right side of the screen, click *Review authorization on root FortiGate*.  
The root FortiGate pop-up window shows the state of the device authorization.

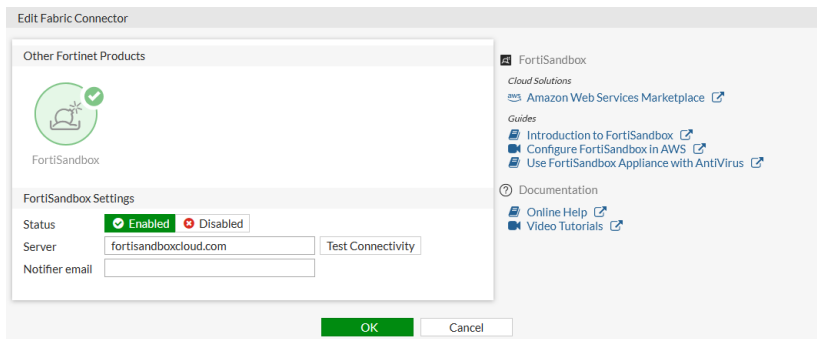
## Use an FQDN in FortiSandbox fabric connectors - 6.4.2

The server field in the FortiSandbox fabric connector supports FQDN addresses.

### To use an FQDN in a FortiSandbox fabric connector in the GUI:

- Go to *Security Fabric > Fabric Connectors*.
- Edit the *FortiSandbox* connector.
- Set *Status* to *Enabled*.

4. Enter the *FQDN* in the *Server* field.



5. Optionally, click *Test Connectivity* to test the connection between the FortiGate and the FQDN. If the FQDN cannot be reached, or if the FortiGate is not authorized on the FortiSandbox, *Unreachable or not authorized* will be displayed.
6. Optionally, enter an email address in the *Notifier email* field.
7. Click *OK*.

**To use an FQDN in a FortiSandbox fabric connector in the CLI:**

```
config system fortisandbox
  set status enable
  set server "fortisandboxcloud.com"
  set source-ip "192.168.1.233"
end
```

## FortiMail Security Fabric integration - 6.4.2

FortiMail can be authorized into the Security Fabric using either the gutter on the *Fabric Connectors* page, or by pre-authorizing using the FortiMail serial number or certificate.

As part of the Security Fabric, FortiMail appears in the Fabric navigation, topologies, widgets, and in the Security Posture report in FortiOS.

**To join the Security Fabric from FortiMail:**

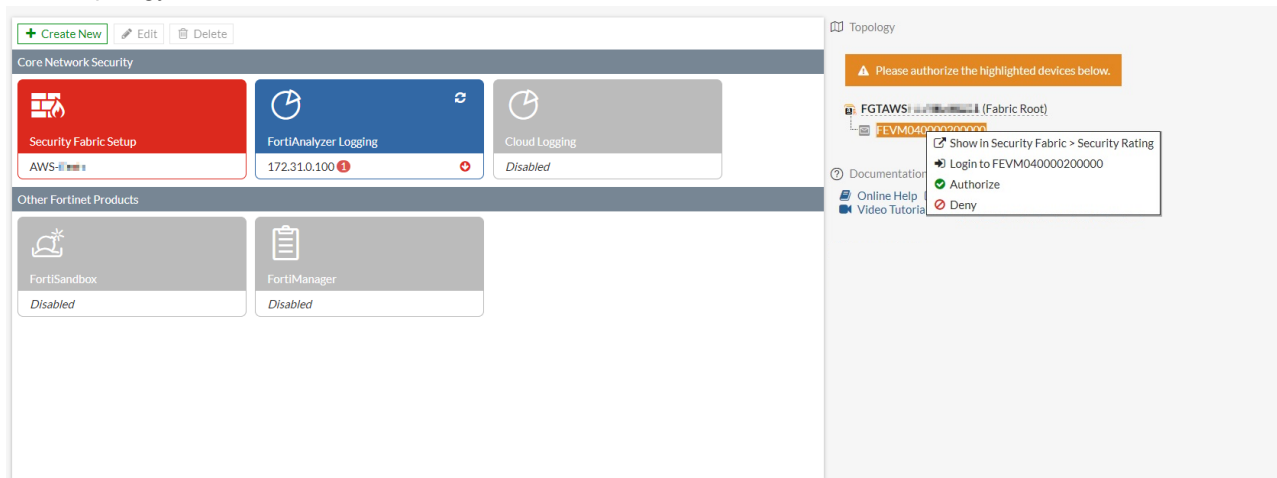
1. Go to *System > Customization* and click the *Corporate Security Fabric* tab (or the *Corporate Security Fabric* tab in FortiMail 6.4.2 and earlier).
2. Click the toggle to enable the Fabric.
3. Enter the *Upstream IP Address* (root FortiGate) and the *Management IP* of the FortiMail.
4. Click *Apply*.

## Authorizing using FortiOS

If the FortiMail was added to the Security Fabric but not pre-authorized, you can authorize it in FortiOS on the *Fabric Connectors* page.

### To authorize FortiMail:

1. Go to *Security Fabric > Fabric Connectors*.
2. In the topology tree, hover over the FortiMail and click *Authorize*.



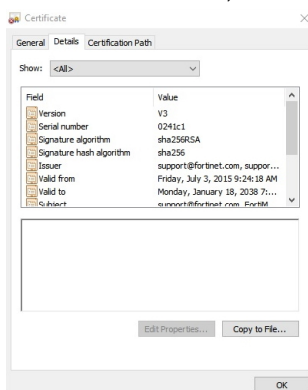
3. Verify the certificate is correct, then click *Accept*.

### Pre-authorizing using the FortiMail certificate

FortiMail can be pre-authorized using its serial number or certificate. When you pre-authorize, the FortiMail can join at any time, and you will not need to authorize it FortiOS. In this example, FortiMail is pre-authorized using a certificate.

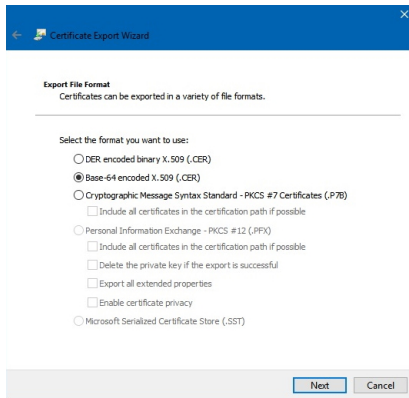
#### To pre-authorize FortiMail using a third-party or default certificate:

1. Log in to FortiMail.
2. Download the certificate. For example, in Chrome:
  - a. In the left side of the address bar, click the icon to view the site information.
  - b. Click *Certificate*.
  - c. Click the *Details* tab, then click *Copy to File*.



- d. The *Certificate Export Wizard* opens. Click *Next* to continue.

- e. For the file format, select *Base-64 encoded X.509 (.CER)*, then click *Next*.



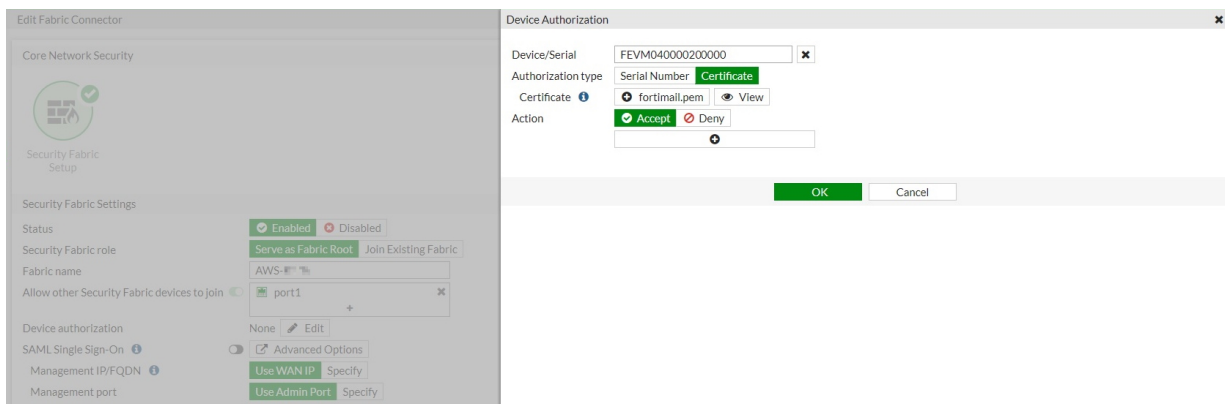
- f. Browse to the folder location and enter a file name, then click *Next*.

- g. Click *Finish*, then click *OK* to close the dialog box.

3. In FortiOS, go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.

4. Beside *Device authorization*, click *Edit* and configure the following:

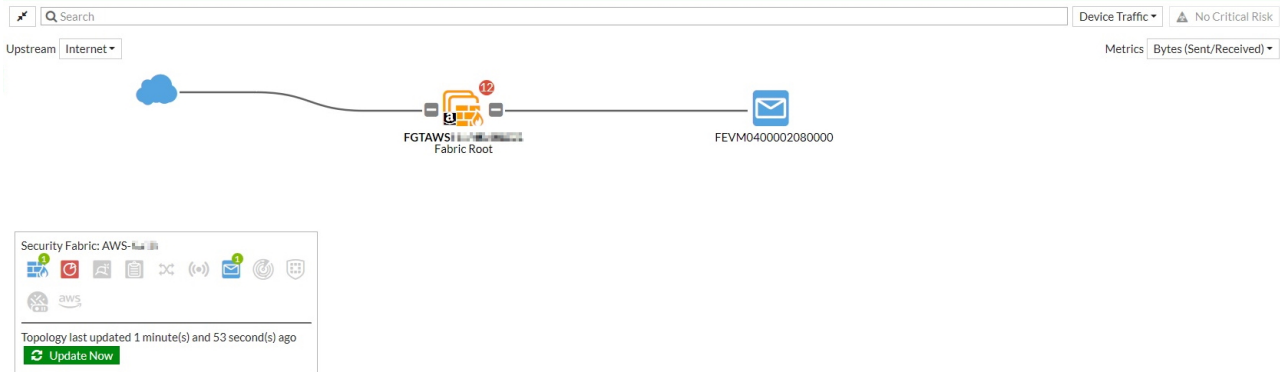
- Enter the FortiMail serial number.
- For *Authorization type*, select *Serial Number*.
- For *Certificate*, upload the .CER file you saved previously.
- Click *OK*.



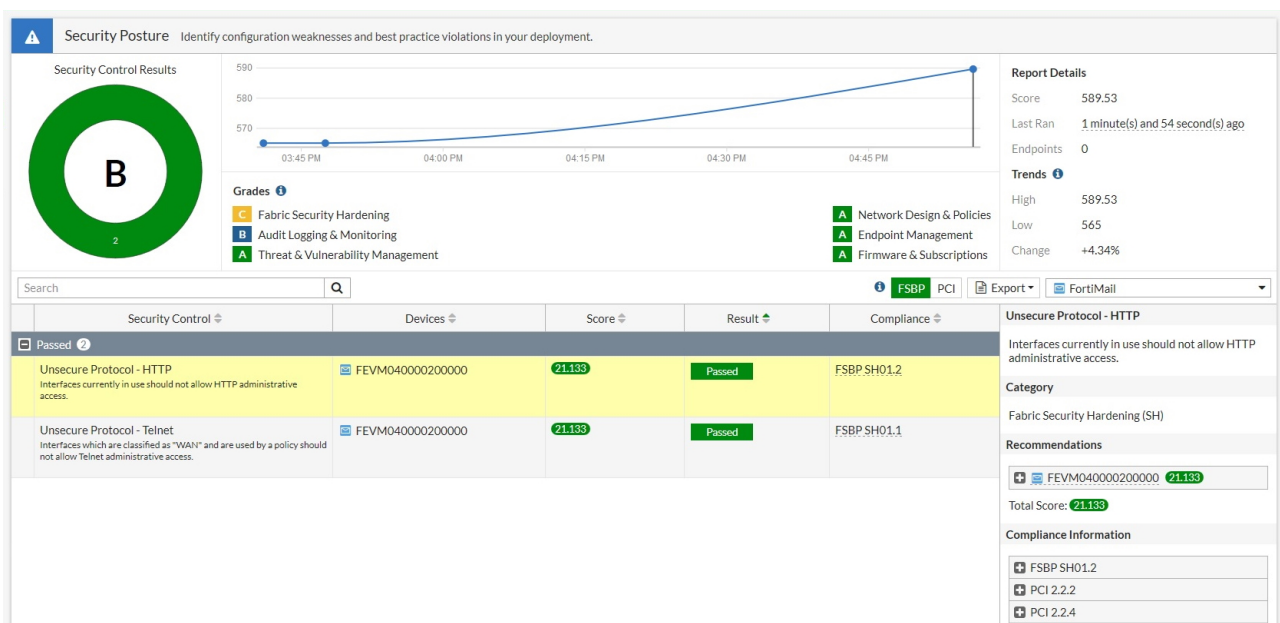
## Security Fabric integration

Once authorized, you can navigate and log in to the FortiMail from the topology tree, or within the topology views in FortiOS:





The Security Posture report can detect whether unsecure protocols, such as HTTP and Telnet, are used on the FortiMail:

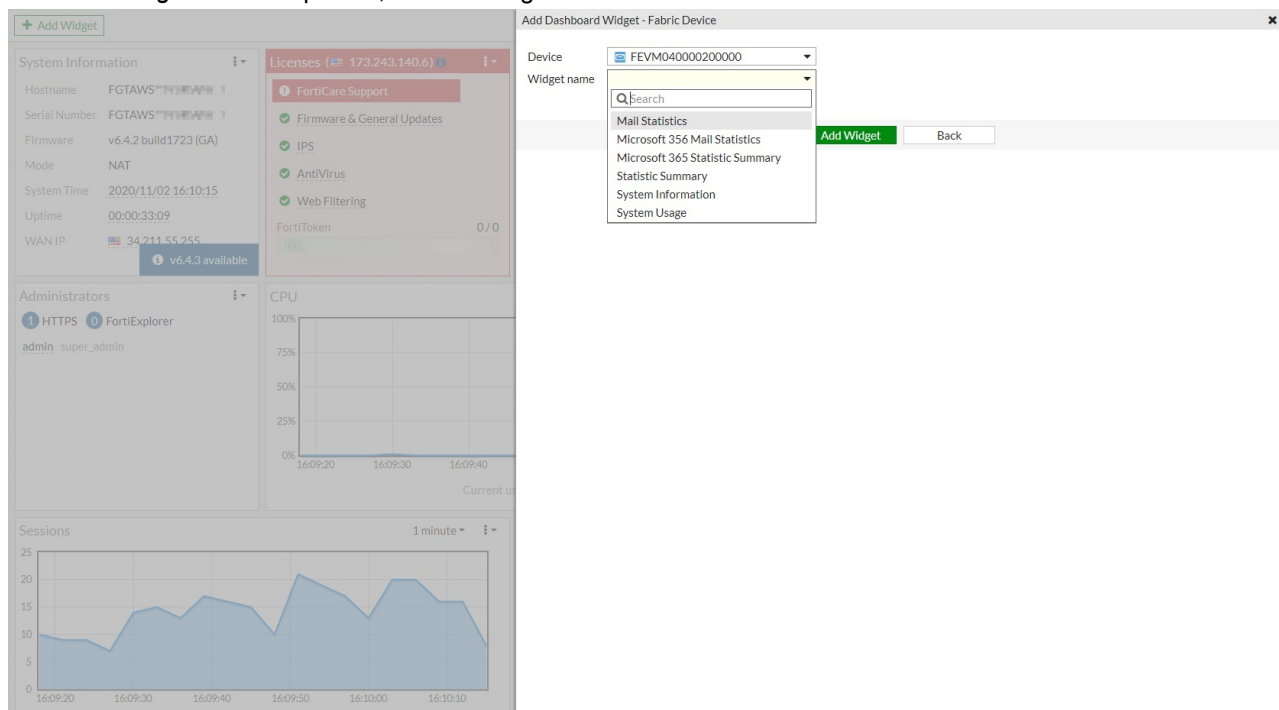


FortiMail widgets can be added to the dashboard.

### To add a FortiMail widget:

1. Go to *Dashboard > Status* and click *Add Widget*. The *Add Dashboard Widget* pane opens.
2. Under *Security Fabric*, click *Fabric Device*.
3. From the *Device* dropdown, select the FortiMail.

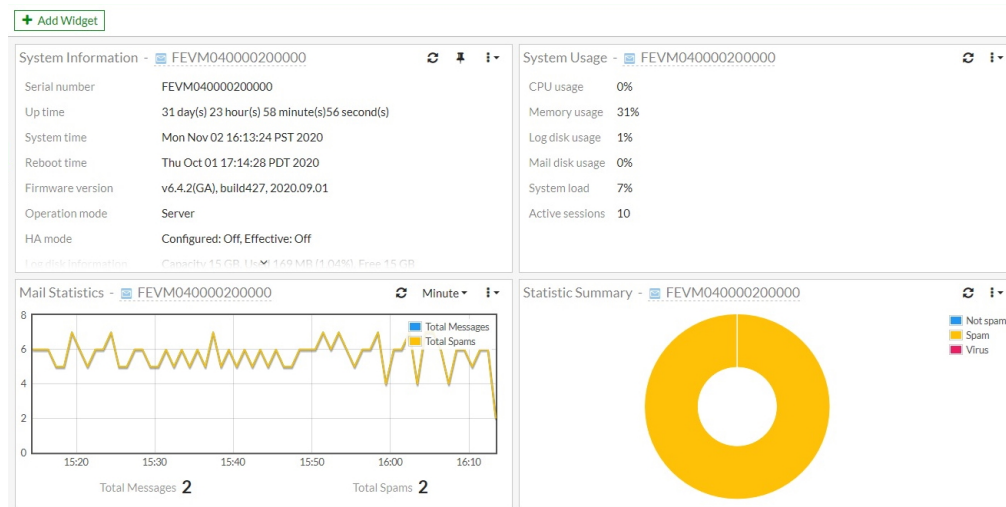
4. From the *Widget name* dropdown, select a widget.



5. Click *Add Widget*.

6. Repeat these steps to add more widgets if needed.

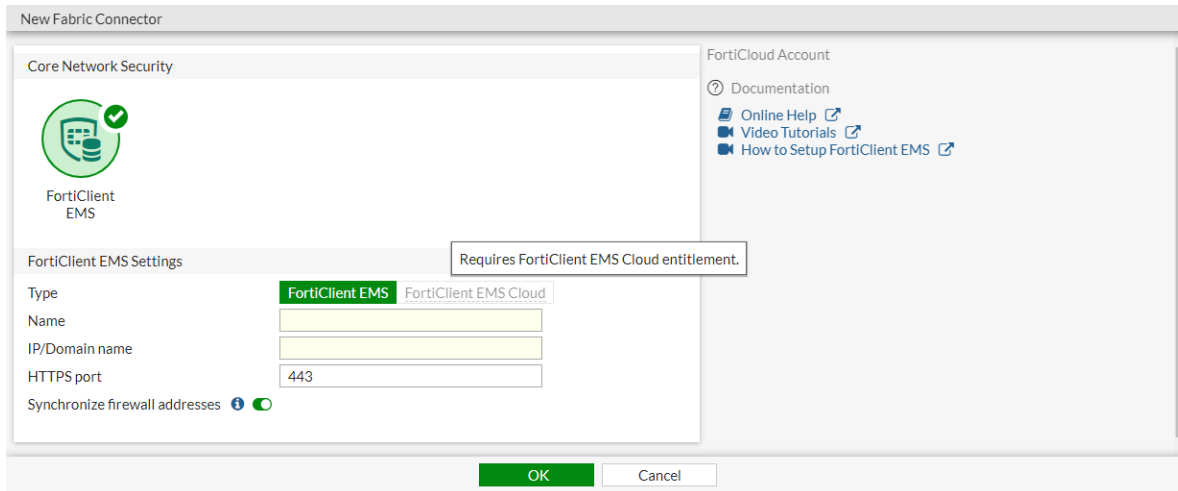
The widgets are displayed in the dashboard:



## Allow EMS Cloud configuration only when the entitlement is verified - 6.4.3

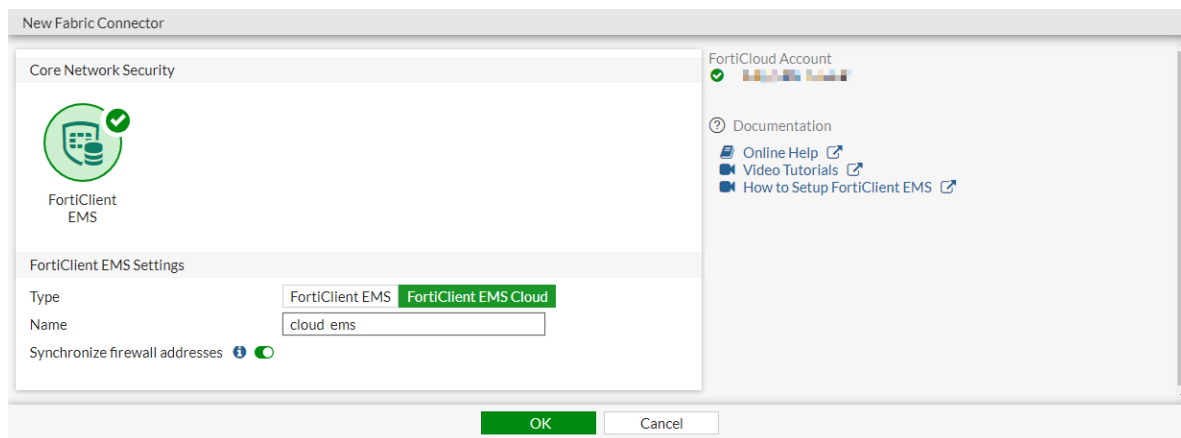
FortiClient EMS Cloud can only be configured when the FortiGate is registered to FortiCloud and the EMS Cloud entitlement is verified.

If the FortiCloud account does not pass the FortiClient EMS Cloud entitlement check, the option is not selectable in the FortiClient EMS connector settings.



### To configure a FortiClient EMS Cloud server Fabric connector in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New* and click *FortiClient EMS*.
3. Set *Type* to *FortiClient EMS Cloud*.
4. Enter a name.



5. Click *OK*.  
A window appears to verify the EMS server certificate.
6. Click *Accept*.  
The *FortiClient EMS Status* section displays a *Successful* connection and an *Authorized* certificate.

### To verify the EMS Cloud entitlement in the CLI:

```
# diagnose test update info
...
Account contracts:
    FCEM,Thu Jan 27 16:00:00 2022
    FCEP,Tue Nov 15 16:00:00 2022
...
Support contract: pending_registration=255 got_contract_info=1
account_id=[test****@*****.com] company=[Fortinet] industry=[Technology]
```

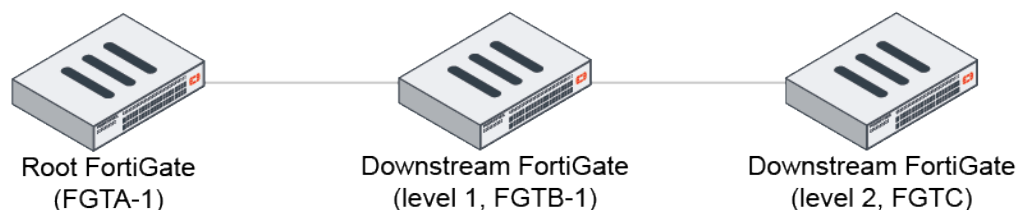
User ID: \*\*\*\*\*

## Improvements to synchronizing objects across the Security Fabric - 6.4.4

The following improvements have been made to synchronize objects across the Security Fabric:

- Set object synchronization (`fabric-object-unification`) to `default` or `local` on a downstream device. When set to `local`, the device does not synchronize objects from the root, but will still participate in sending the synchronized object downstream.
- Add a per object option to toggle whether the specific Fabric object will be synchronized or not. After upgrading from 6.4.3, this option is disabled for supported Fabric objects. The synchronized Fabric objects are kept as locally created objects on downstream FortiGates.
- Simplify the conflict resolution procedure.
- Allow FortiGates to define the number of task workers to handle synchronizations.

### Sample topology



In this Security Fabric, the root FortiGate (FGTA-1) has `fabric-object-unification` set to `default` so the Fabric objects can be synchronized to the downstream FortiGate. The level 1 downstream FortiGate (FGTB-1) has `configuration-sync` set to `local`, so it will not apply the synchronized objects locally. The level 2 downstream FortiGate (FGTC) has `configuration-sync` set to `default`, so it will apply the synchronized objects locally.

In this example, firewall addresses and address groups are used. Other supported Fabric objects have the same behaviors. The following use cases illustrate the synchronization improvements:

- If no conflicts exist, firewall addresses and address groups can be synchronized to downstream FortiGates ([see example below](#)).
- If a conflict exists between the root and downstream FortiGates, it can be resolved with the conflict resolution wizard. After the conflict is resolved, the firewall addresses and address groups can be synchronized to downstream FortiGates ([see example below](#)).
- If `set fabric-object` (*Fabric synchronization* option in the GUI) is disabled for firewall addresses and address groups on the root FortiGate, they will not be synchronized to downstream FortiGates ([see example below](#)).

### To configure the FortiGates used in this example:

```

FGTA-1 # config system csf
    set status enable
    set group-name "csf_script"
    set fabric-object-unification default
    ...
end
  
```

```
FGTB-1 # config system csf
    set status enable
    set upstream-ip 10.2.200.1
    set configuration-sync local
    ...
end

FGTC # config system csf
    set status enable
    set upstream-ip 192.168.7.2
    set configuration-sync default
    ...
end
```

### To synchronize a firewall address and address group in the Security Fabric:

#### 1. Configure the firewall address on the root FortiGate:

```
FGTA-1 # config firewall address
    edit "add_subnet_1"
        set fabric-object enable
        set subnet 22.22.22.0 255.255.255.0
    next
end
```

#### 2. Configure the address group on the root FortiGate:

```
FGTA-1 # config firewall addrgrp
    edit "group_subnet_1"
        set member "add_subnet_1"
        set fabric-object enable
    next
end
```

#### 3. Check the firewall address and address group on the downstream FortiGates:

```
FGTB-1 # show firewall address add_subnet_1
entry is not found in table

FGTB-1 # show firewall addrgrp group_subnet_1
entry is not found in table
```

The synchronized objects are not applied locally on this FortiGate because `configuration-sync` is set to `local`.

```
FGTC # show firewall address add_subnet_1
config firewall address
    edit "add_subnet_1"
        set uuid 378a8094-34cb-51eb-ce40-097f298fcfdc
        set fabric-object enable
        set subnet 22.22.22.0 255.255.255.0
    next
end

FGTC # show firewall addrgrp group_subnet_1
config firewall addrgrp
    edit "group_subnet_1"
        set uuid 4d7a8a52-34cb-51eb-fce7-d93f76915319
        set member "add_subnet_1"
```

```

        set color 19
        set fabric-object enable
    next
end

```

The objects are synchronized on this FortiGate because `configuration-sync` is set to default.

### To resolve a firewall address and address group conflict in the Security Fabric:

1. On FGTC, create a firewall address:
  - a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
  - b. Configure the following:

Name	sync_add_1
IP/Netmask	33.33.33.0 255.255.255.0

Edit Address

Category
Address
IPv6 Address
Multicast Address
Proxy Address

Name
sync\_add\_1

Color
Change

Type
Subnet

IP/Netmask
33.33.33.0 255.255.255.0

Interface
any

Static route configuration

Comments
Write a comment... 0/255

FortiGate
FGTC
Dynamic Address
Guides
Configuring an AWS Dynamic Address
Configuring an Azure Dynamic Address
Configuring a Google Cloud Platform Dynamic Address
Configuring an Oracle Cloud Infrastructure Dynamic Address
Configuring an OpenStack Dynamic Address
Documentation
Online Help
Video Tutorials

OK
Cancel

- c. Click OK.
2. On FGTA-1 (Fabric root), create the firewall address with same name but a different subnet:
  - a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
  - b. Configure the following:

Name	sync_add_1
IP/Netmask	11.11.11.0 255.255.255.0
Fabric synchronization	Enable

c. Click **OK**.

3. Add the address to a different address group than what is configured on FGTC:

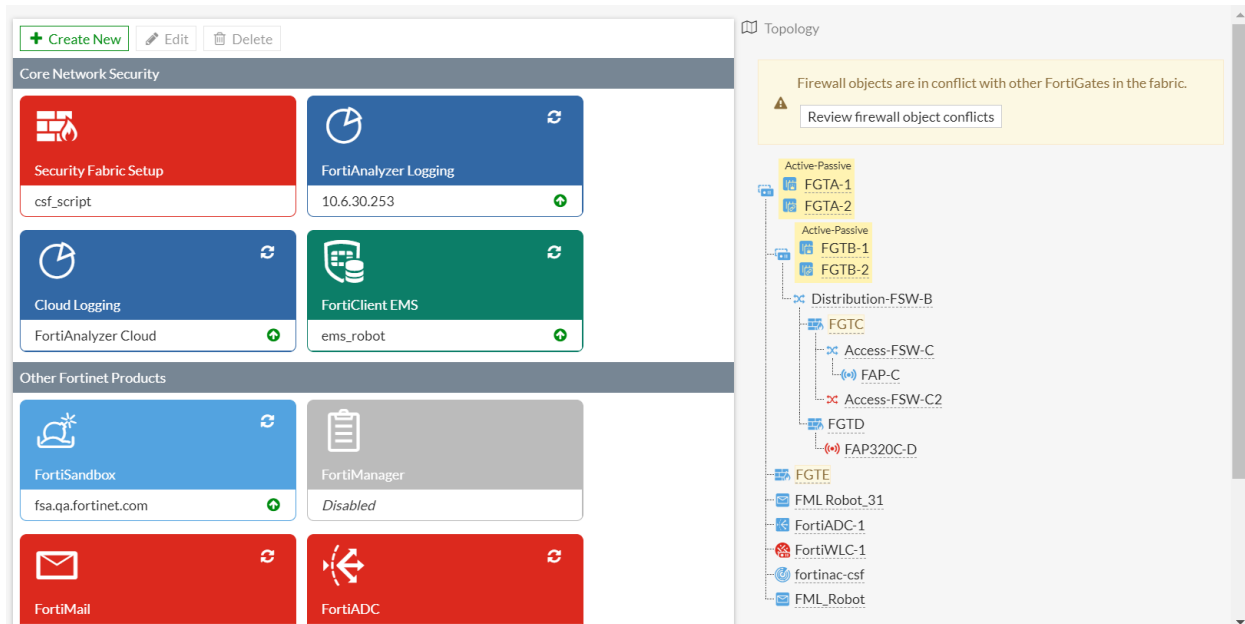
a. Go to **Policy & Objects > Addresses** and click **Create New > Address Group**.

b. Configure the following:

Name	sync_group4
Members	sync_add_1
Fabric synchronization	Enable

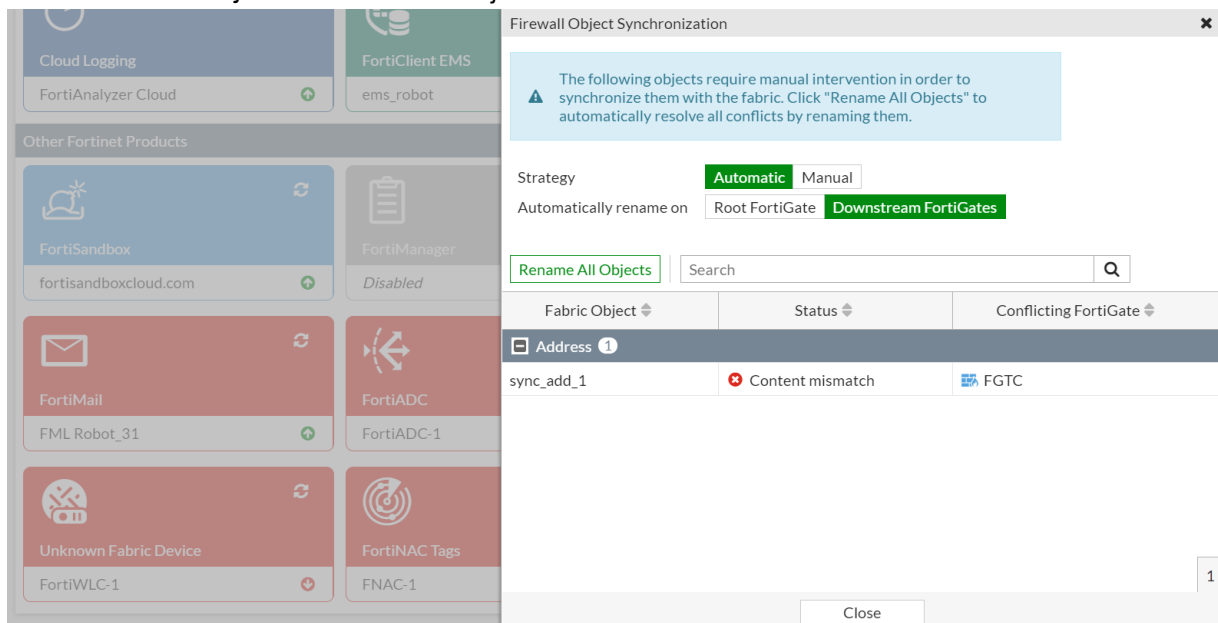
c. Click **OK**.

4. Go to **Security Fabric > Fabric Connectors**. In the topology tree, there is a message that *Firewall objects are in conflict with other FortiGates in the fabric*.



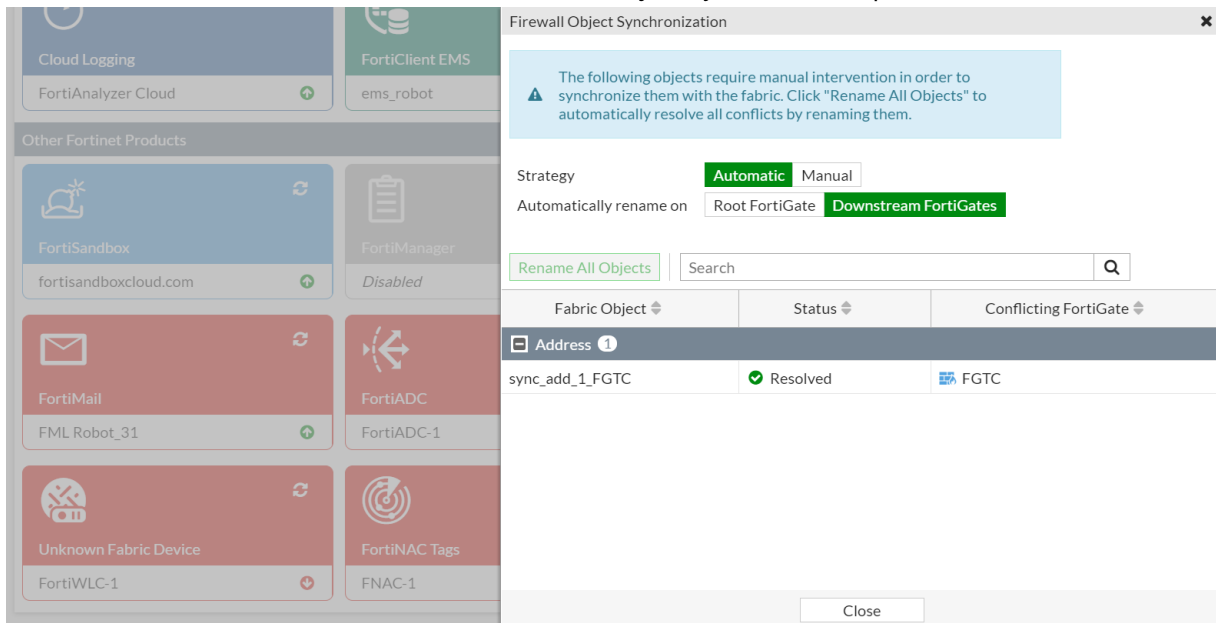
5. Resolve the conflict:

- Click *Review firewall object conflicts*. The *Firewall Object Synchronization* pane opens.
- Click *Rename All Objects*. The conflicted object will be renamed on the downstream FortiGate.

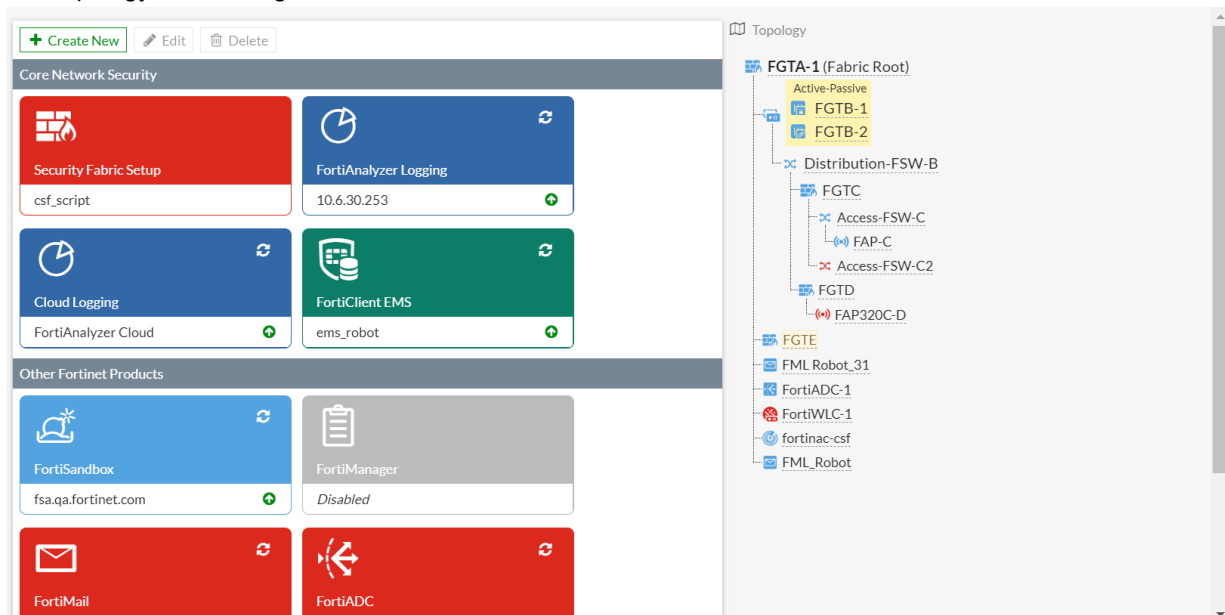




- c. The conflict is resolved. Click *Close* to exit the *Firewall Object Synchronization* pane.



- d. The topology tree no longer indicates there is a conflict.



6. Verify the results on the downstream FortiGates:

- On FGTB-1, go to *Policy & Objects > Addresses*.
- Search for *sync\_add\_1* and *sync\_group4*. No results are found. The synchronized objects are not applied locally on this FortiGate because *configuration-sync* is set to *local*.



<a href="#">+ Create New</a>	<a href="#">Edit</a>	<a href="#">Clone</a>	<a href="#">Delete</a>	<input type="text" value="sync_group4"/>	<a href="#">×</a>	<a href="#">Q</a>
Name	Details	Interface	Type	Ref.	No results	

- c. On FGTC, go to *Policy & Objects > Addresses*.
- d. Search for *sync\_add\_1*. The original firewall address *sync\_add\_1* was renamed to *sync\_add\_1\_FGTC* by resolving the conflict on FGTA-1. The address *sync\_add\_1* and address group *sync\_group4* are synchronized from FGTA-1.

<div><div>+ Create New</div><div>Edit</div><div>Clone</div><div>Delete</div></div>		<div>sync_add_1</div> <div><div>✕</div><div>Q</div></div>		<div><div>?</div></div>					
Name		Details		Interface		Type		Ref.	
IP Range/Subnet 2/6									
sync_add_1		11.11.11.0/24				Address		1	
sync_add_1_FGTC		33.33.33.0/24				Address		0	
Address Group 1									
sync_group4		sync_add_1				Address Group		0	

### To disable Fabric synchronization on the root FortiGate in the GUI:

1. On FGTA-1, create a firewall address:
  - a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
  - b. Configure the following:

Name	add_subnet_3
IP/Netmask	33.33.33.0 255.255.255.0
Fabric synchronization	Disable

- c. Click *OK*.
2. Create the firewall address group and add the address:
  - a. Go to *Policy & Objects > Addresses* and click *Create New > Address Group*.
  - b. Configure the following:

Name	group_subnet_3
Members	add_subnet_3
Fabric synchronization	Disable

- c. Click *OK*.
3. On FGTC, go to *Policy & Objects > Addresses* and search for *subnet\_3*. No results are found because Fabric synchronization is disabled on the root FortiGate (FGTA-1).

<a href="#">+ Create New</a>	<a href="#">Edit</a>	<a href="#">Clone</a>	<a href="#">Delete</a>	<input type="text" value="subnet_3"/>	<a href="#">×</a>	<a href="#">Q</a>	<a href="#">i</a>
Name	Details	Interface	Type	Ref.	No results		

4. On FGTC, go to *Policy & Objects > Addresses* and search for *subnet\_3*. No results are found because Fabric

synchronization is disabled on the root FortiGate (FGTA-1).

<div> <div>+ Create New</div> <div>Edit</div> <div>Clone</div> <div>Delete</div> <div>subnet_3</div> <div>x</div> <div>Q</div> </div> <div></div>				
Name	Details	Interface	Type	Ref.
No results				

## To disable Fabric synchronization on the root FortiGate in the CLI:

1. Configure the firewall address on the root FortiGate:

```
FGTA-1 # config firewall address
edit "add_subnet_3"
set subnet 33.33.33.0 255.255.255.0
set fabric-object disable
next
end
```

2. Configure the address group on the root FortiGate:

```
FGTA-1 # config firewall addrgrp
edit "group_subnet_3"
set member "add_subnet_3"
set fabric-object disable
next
end
```

3. Check the firewall address and address group on the downstream FortiGates:

```
FGTB-1 # show firewall address add_subnet_3
entry is not found in table

FGTB-1 # show firewall addrgrp group_subnet_3
entry is not found in table

FGTC # show firewall address add_subnet_3
entry is not found in table

FGTC # show firewall addrgrp group_subnet_3
entry is not found in table
```

The objects are not synchronized from the root FortiGate (FGTA-1) because the `fabric-object` setting is disabled.

## Detect FortiManager Cloud account level subscription - 6.4.4

If a FortiCloud account has a FortiManager Cloud account level subscription (ALCI), a FortiGate registered to the FortiCloud account can recognize it and enable FortiManager Cloud central management.

### To configure FortiManager Cloud central management:

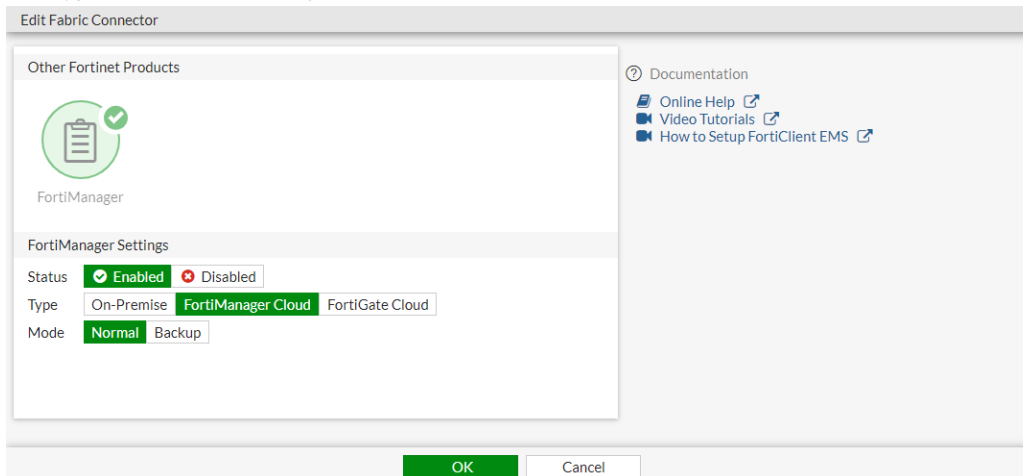
1. Register the FortiGate (see [Registration](#)). If the FortiCare account has a FortiManager Cloud contract (10 device limitation), the FortiGate is allowed to enable FortiManager Cloud.
2. In FortiOS, verify the contract information to check the contract is valid:

```
# diagnose test update info contract
...
```

```
System contracts:
...
Account contracts:
  FMGC,Thu Dec  2 16:00:00 2021
...
```

### 3. Enable FortiManager Cloud:

- Go to *Security Fabric > Fabric Connectors* and double-click the *FortiManager* card.
- For *Type*, select *FortiManager Cloud*.

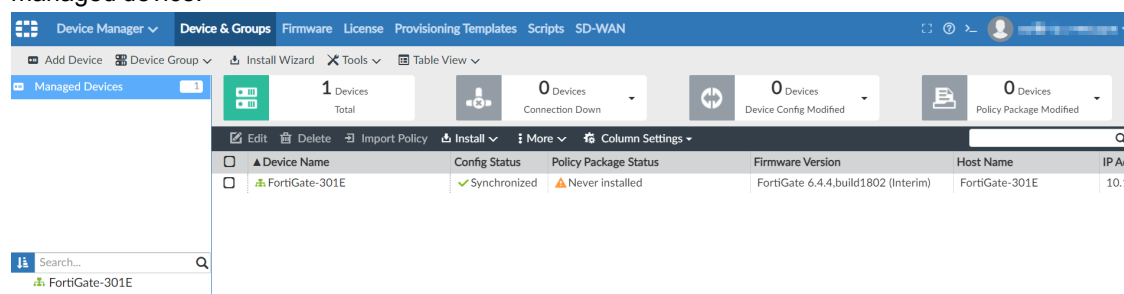


- Click **OK**.

### 4. Verify the FortiManager Cloud status:

```
# diagnose fdsm central-mgmt-status
Connection status: Handshake
Registration status: Unknown
```

- In the FortiCloud portal, click the dropdown beside your user name and select *Cloud Management > FortiManager*.
- Click the corresponding account to launch the FortiManager Cloud instance.
- In FortiManager Cloud, go to *Device Manager > Device & Groups*. The FortiGate is now listed as synchronized managed device.



### 8. In FortiOS, verify the FortiManager Cloud status again:

```
# diagnose fdsm central-mgmt-status
Connection status: Up
Registration status: Registered
```

## SDN connectors

This section includes information about SDN connector related new features:

- [SDN connector for Cisco ACI northbound API integration on page 71](#)
- [Support multiple SDN connector instances for Cisco ACI and Nuage on page 74](#)
- [Multifunction tooltip for Fabric connectors on page 81](#)
- [Exchange Server connector with Kerberos KDC auto-discovery on page 82](#)
- [Support IBM Cloud SDN connector 6.4.1 on page 83](#)
- [Support ServiceTag and Region for Azure SDN connector address objects 6.4.2 on page 87](#)
- [Multiple IP addresses on Cisco ACI connectors 6.4.4 on page 89](#)
- [Multiple clusters on Cisco ACI connectors 6.4.9 on page 93](#)
- [Update OpenStack SDN connector to support the latest OpenStack releases 6.4.9 on page 96](#)

### SDN connector for Cisco ACI northbound API integration

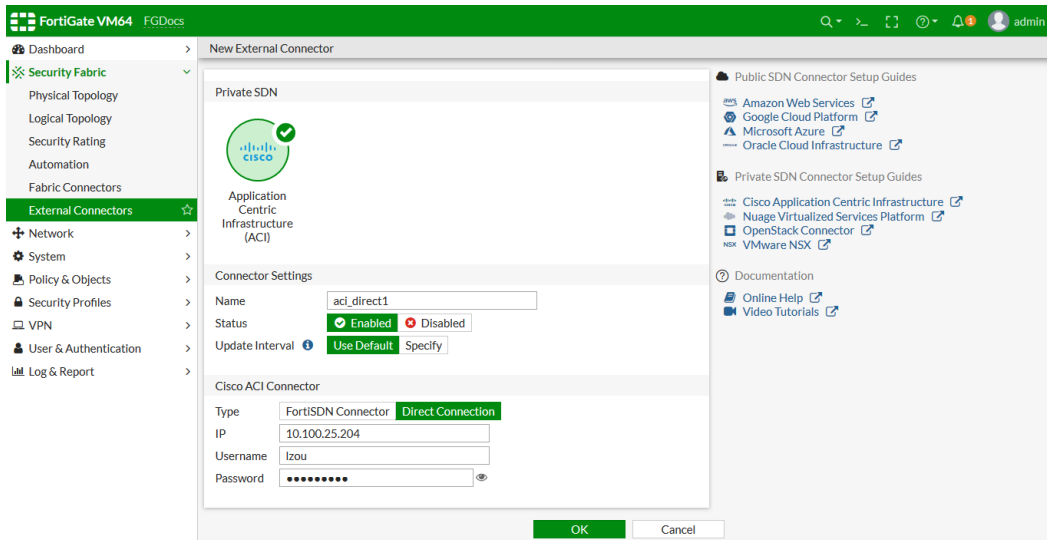
A new SDN connector type has been added for Cisco ACI (Application Centric Infrastructure) northbound API integration. Administrators can define a dynamic firewall addresses for Cisco ACI directly. Deploying an SDN connector through an external VM between the FortiGate and Cisco ACI is no longer required.

The following address filters are supported:

- Tenant
- Application
- Endpoint group
- Tag

#### To configure a Cisco ACI connector in the GUI:

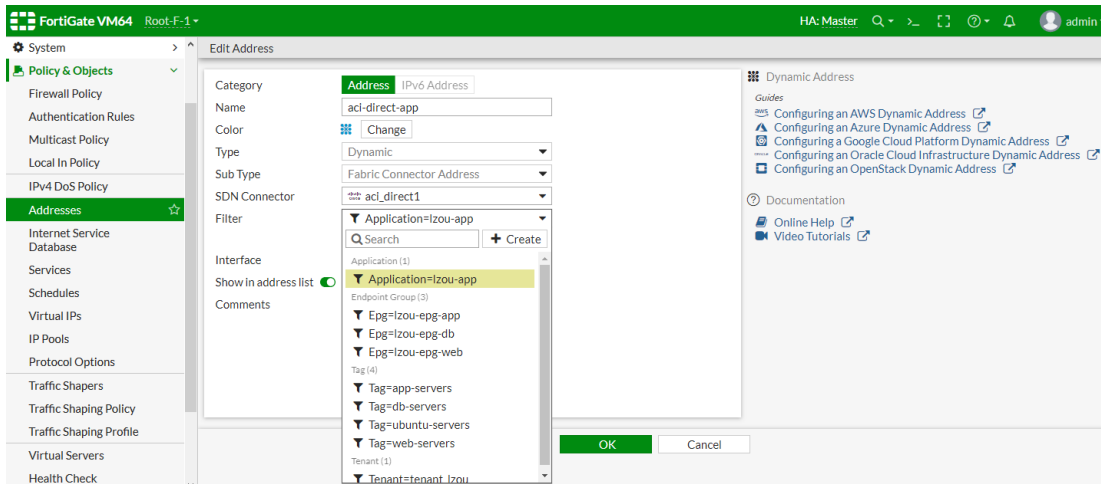
1. Configure the Cisco ACI SDN connector:
  - a. Go to *Security Fabric > External Connectors*.
  - b. Click *Create New*, and select *Application Centric Infrastructure (ACI)*.
  - c. Configure the *Connector Settings* as needed. The update interval is in seconds.
  - d. In the *Cisco ACI Connector* section, for *Type*, select *Direct Connection* and configure the remaining settings based on your deployment.



e. Click OK.

2. Create a dynamic firewall address for the connector:

- a. Go to *Policy & Objects > Addresses*.
- b. Click *Create New > Address* and enter a name.
- c. Configure the following settings:
  - i. For *Type*, select *Dynamic*.
  - ii. For *Sub Type*, select *Fabric Connector Address*.
  - iii. For *SDN Connector*, select the connector created in step 1.
  - iv. For *Filter*, select an entry from the dropdown list. In this example, *Application* is selected.



d. Click OK.

### 3. Confirm that the connector resolves the dynamic firewall IP addresses:

- Go to *Policy & Objects > Addresses*.
- In the address table, hover over the address created in step 2 to view which IPs it resolves to:

Name	Type	Details	Interface	Visibility	Ref.
aci-add-tag	Dynamic (ACI)			Visible	0
aci-direct-app	Dynamic (ACI-DIRECT)			Visible	0
aci-direct-end	Dynamic (ACI-DIRECT)			Visible	0
aci-direct-tag	Dynamic (ACI-DIRECT)			Visible	0
aci-direct-ten	Dynamic (ACI-DIRECT)			Visible	0
all-address-se	Dynamic (ALICLOUD)			Visible	0
all	Subnet	0.0.0.0/0		Visible	17
autoupdate.o	FQDN	autoupdate.opera.com		Visible	2
aws-address-tag-1	Dynamic (AWS)			Visible	0
aws-address-tag-2	Dynamic (AWS)			Visible	0
aws-address-wildcard	Dynamic (AWS)			Visible	0
aws-autoscale-1	Dynamic (AWS)			Visible	0
azure_add1	Dynamic (AZURE)			Visible	0
charlie_test	Dynamic (NSX)			Visible	0
csf_ns_group	Dynamic (NSX)			Visible	0
fgt	Dynamic (NSX)			Visible	0
gcp-address-node-1	Dynamic (GCP)			Visible	0
gcp-address-node-2	Dynamic (GCP)			Visible	0
gcp-address-wildcard	Dynamic (GCP)			Visible	0
gcp-ops	Dynamic (GCP)			Visible	0

### To configure a Cisco ACI connector in the CLI:

#### 1. Configure the Cisco ACI SDN connector:

```
config system sdn-connector
  edit "aci_direct1"
    set status enable
    set type aci-direct
    set server "10.100.25.204"
    set username "lzou"
    set password xxxxxxxx
    set update-interval 60
  next
end
```

#### 2. Create a dynamic firewall address for the connector:

```
config firewall address
  edit "aci-direct-app"
    set type dynamic
    set sdn "aci_direct1"
    set color 17
    set filter "Application=lzou-app"
  next
end
```

#### 3. Confirm that the connector resolves the dynamic firewall IP addresses:

```
config firewall address
  edit "aci-direct-app"
    show
      config firewall address
        edit "aci-direct-app"
```

```
set uuid 794aaf20-3e33-51ea-57e1-10b5badf3fc7
set type dynamic
set sdn "aci_direct1"
set color 17
set filter "Application=lzou-app"
config list
  edit "10.0.5.11"
  next
  edit "10.0.5.12"
  next
  edit "10.0.6.11"
  next
  edit "10.0.6.12"
  next
  edit "10.0.6.13"
  next
  edit "10.0.6.14"
  next
  edit "10.0.7.11"
  next
  edit "10.0.7.12"
  next
end
next
end
next
end
```

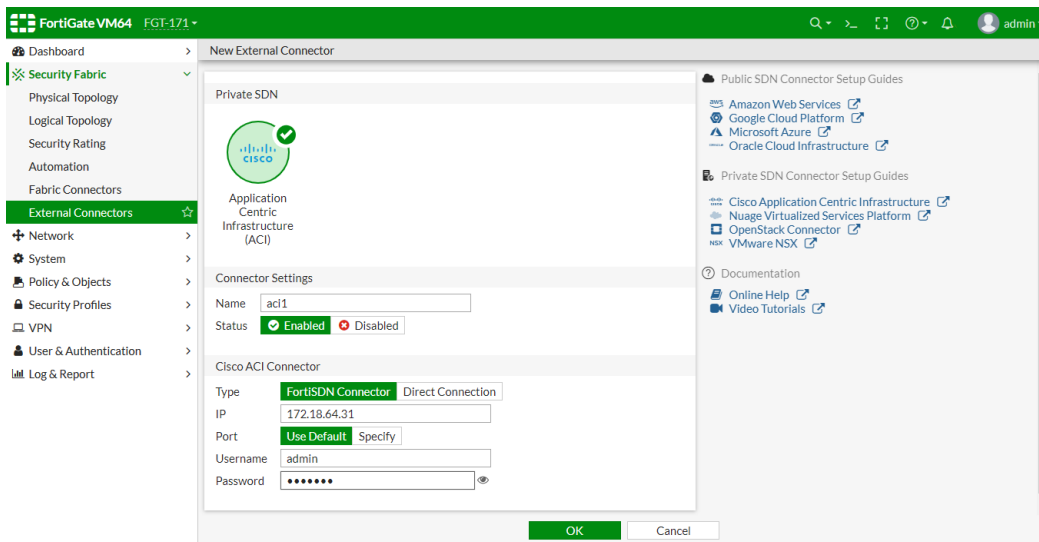
## Support multiple SDN connector instances for Cisco ACI and Nuage

Users can configure multiple Cisco ACI (Application Centric Infrastructure) and Nuage SDN connectors, which can be used in dynamic firewall addresses. The following examples configure two Cisco ACI and two Nuage SDN connectors.

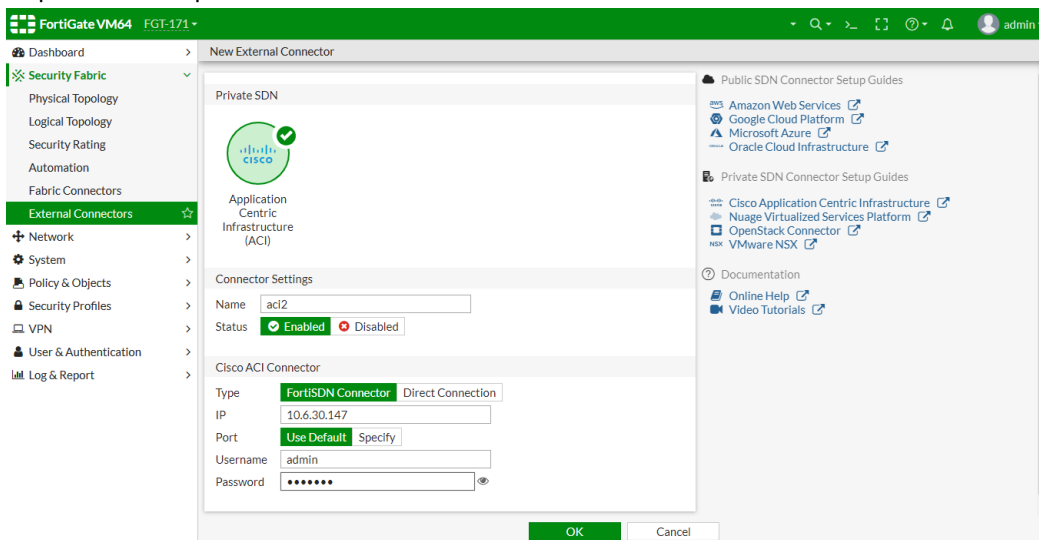
### To configure Cisco ACI connectors in the GUI:

1. Configure the Cisco ACI SDN connectors:
  - a. Go to *Security Fabric > External Connectors* and click *Create New*.
  - b. In the *Private SDN* section, click *Application Centric Infrastructure (ACI)*.
  - c. In the *Cisco ACI Connector* section, for *Type*, select *Fortinet SDN Connector* and configure the remaining settings as needed.

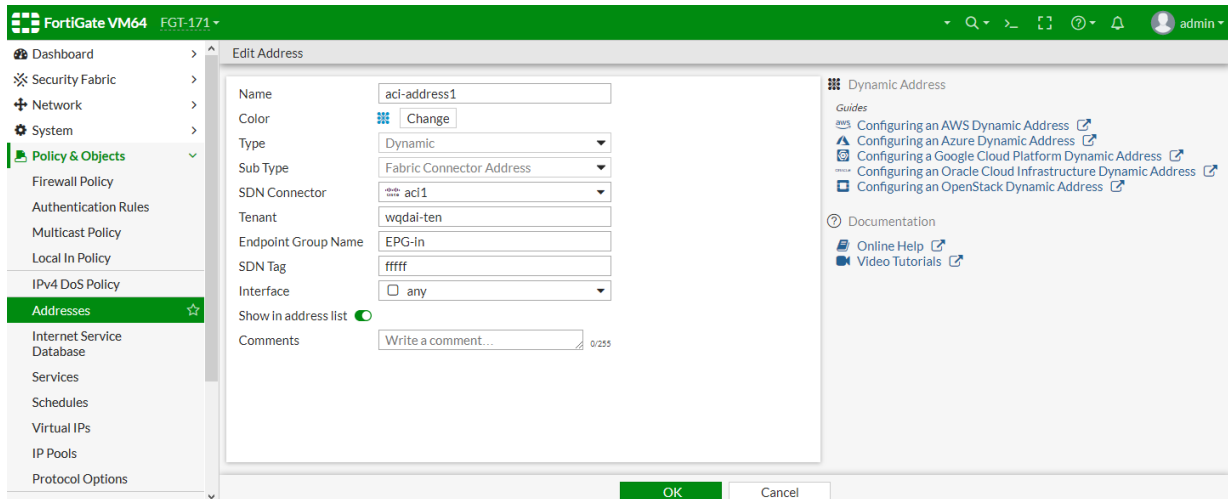




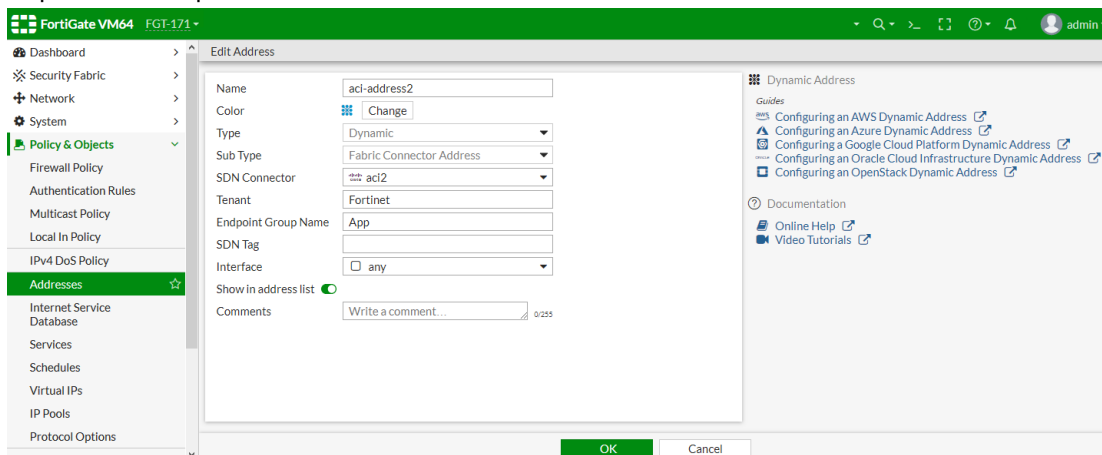
- d. Click OK.
- e. Repeat these steps for the second connector.



2. Create dynamic firewall addresses for the connectors:
  - a. Go to **Policy & Objects > Addresses** and click **Create New > Address**.
  - b. Configure the following settings:
    - i. For **Type**, select **Dynamic**.
    - ii. For **Sub Type**, select **Fabric Connector Address**.
    - iii. For **SDN Connector**, select the first ACI connector.
    - iv. Configure the remaining settings as needed.



- c. Click OK.
- d. Repeat these steps for the second connector.



### To configure Nuage connectors in the GUI:

1. Configure the Nuage SDN connectors:
  - a. Go to *Security Fabric > External Connectors* and click *Create New*.
  - b. In the *Private SDN* section, click *Nuage Virtualized Services Platform*.

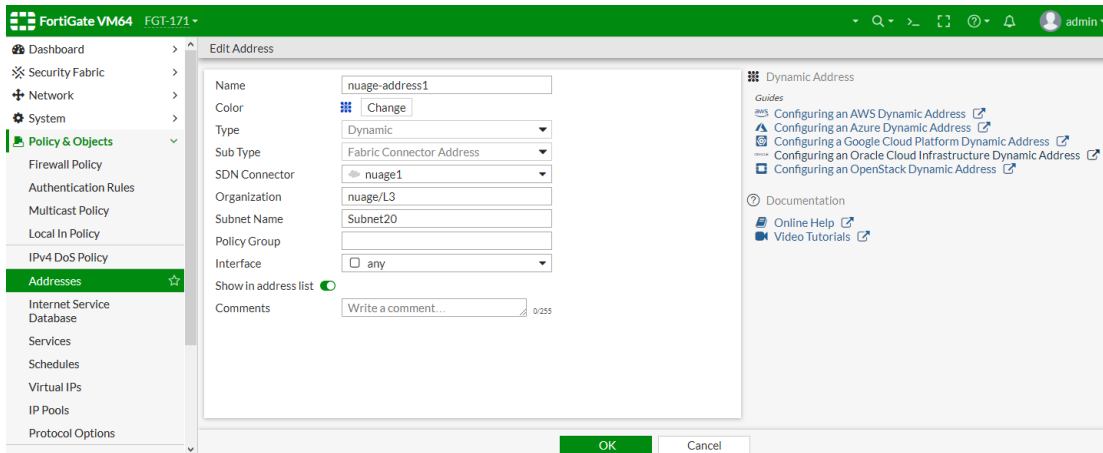
## c. Configure the settings as needed.

## d. Click OK.

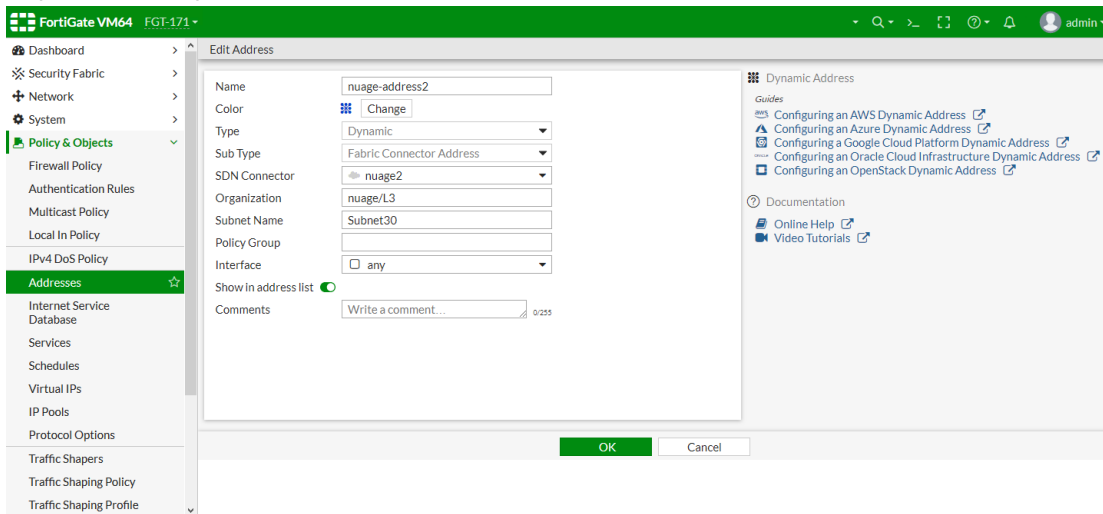
## e. Repeat these steps for the second connector.

## 2. Create dynamic firewall addresses for the connectors:

- a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
- b. Configure the following settings:
  - i. For *Type*, select *Dynamic*.
  - ii. For *Sub Type*, select *Fabric Connector Address*.
  - iii. For *SDN Connector*, select the first the first Nuage connector.
  - iv. Configure the remaining settings as needed.



- c. Click OK.
- d. Repeat these steps for the second connector.



## To verify the dynamic firewall IPs are resolved by the SDN connector in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. In the address table, hover over an address to view which IPs it resolves to:

Name	Type	Details	Interface	Visibility	Ref.
<b>Address 15</b>					
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_A	Subnet	0.0.0.0/0		Hidden	0
SSLVPN_TUN	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	2
aci-address1	Dynamic (ACI)			Visible	0
aci-address2	Dynamic (ACI)			Visible	0
all	Subnet	0.0.0.0/0		Visible	0
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0
nuage-address1	Dynamic (NUAGE)			Visible	0
nuage-address2	Dynamic (NUAGE)			Visible	0
wildcard.dropbox.com	FQDN	*dropbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	1

## To configure Cisco ACI connectors in the CLI:

1. Configure the SDN connectors:

```
config system sdn-connector
  edit "aci1"
    set type aci
    set server "172.18.64.31"
    set username "admin"
    set password xxxxxxxx
  next
  edit "aci2"
    set type aci
    set server "10.6.30.147"
    set username "admin"
    set password xxxxxxxx
  next
end
```

2. Create dynamic firewall addresses for the connectors:

```
config firewall address
  edit "aci-address1"
    set type dynamic
    set sdn "aci1"
    set color 17
    set tenant "wqdai-ten"
    set epg-name "EPG-in"
    set sdn-tag "fffff"
  next
  edit "aci-address2"
    set type dynamic
    set sdn "aci2"
    set color 17
```

```
        set tenant "Fortinet"
        set epd-name "App"
    next
end
```

## To configure Nuage connectors in the CLI:

### 1. Configure the SDN connectors:

```
config system sdn-connector
    edit "nuage1"
        set type nuage
        set server "172.18.64.27"
        set server-port 5671
        set username "admin"
        set password xxxxxxxx
    next
    edit "nuage2"
        set type nuage
        set server "10.6.30.134"
        set server-port 5671
        set username "admin"
        set password xxxxxxxx
    next
end
```

### 2. Create dynamic firewall addresses for the connectors:

```
config firewall address
    edit "nuage-address1"
        set type dynamic
        set sdn "nuage1"
        set color 19
        set organization "nuage/L3"
        set subnet-name "Subnet20"
    next
    edit "nuage-address2"
        set type dynamic
        set sdn "nuage2"
        set color 19
        set organization "nuage/L3"
        set subnet-name "Subnet30"
    next
end
```

## To verify the dynamic firewall IPs are resolved by the SDN connector in the CLI:

```
# diagnose firewall dynamic list
```

List all dynamic addresses:

```
aci1.aci.wqdai-ten.EPG-in.fffff: ID(171)
    ADDR(192.168.100.20)
```

```
nuage1.nuage.nuage/L3.Subnet20.*: ID(196)
    ADDR(192.168.20.92)
    ADDR(192.168.20.240)
```

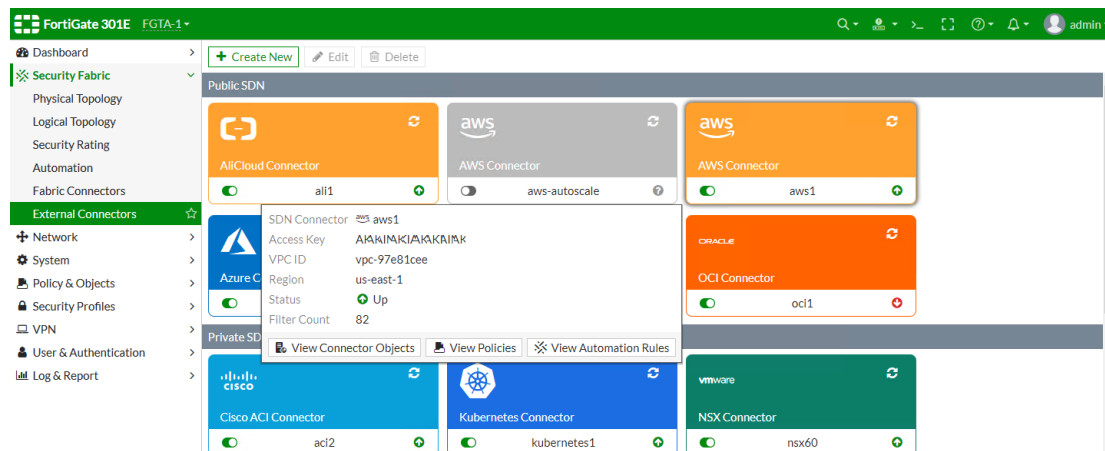
```
nuage2.nuage.nuage/L3.Subnet30.*: ID(198)
  ADDR(192.168.30.92)
```

```
aci2.aci.Fortinet.App.*: ID(218)
  ADDR(150.0.0.10)
  ADDR(192.168.21.11)
  ADDR(192.168.2.100)
```

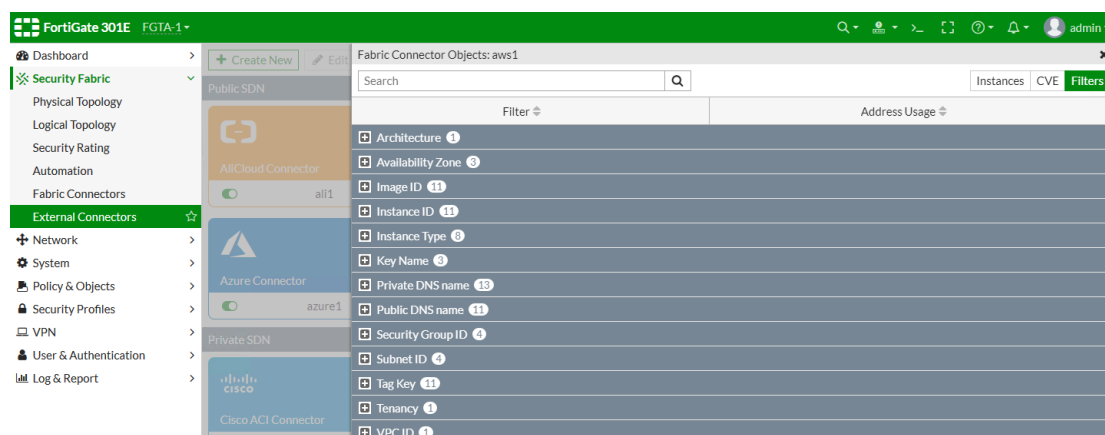
## Multifunction tooltip for Fabric connectors

FortiOS 6.4.0 adds tooltips to Fabric connector cards and other areas that reference the Fabric connector. Tooltips provide information on the connector, associated actions, and policies and objects defined against the connectors, driven primarily from tooltips throughout FortiOS.

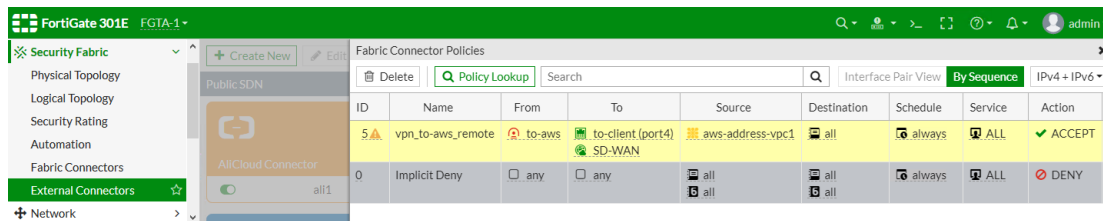
In *Security Fabric > External Connectors*, when you hover over a Fabric connector, a tooltip appears that shows basic information on its configuration.



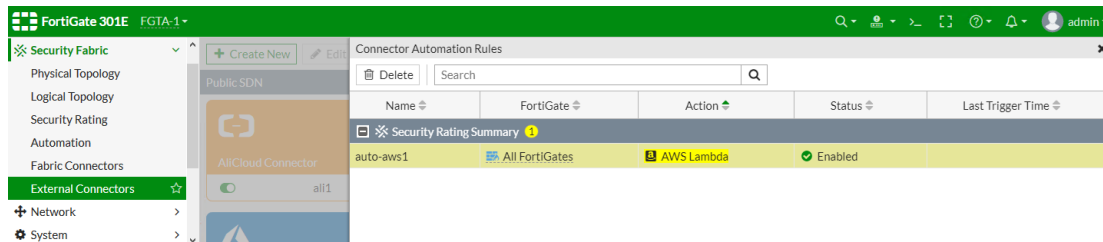
If you click *View Connector Objects* from this tooltip, the *Fabric Connector Objects* pane shows this Fabric connector's dynamic objects, such as filters. For an AWS Fabric connector, this pane also shows instance and CVE information.



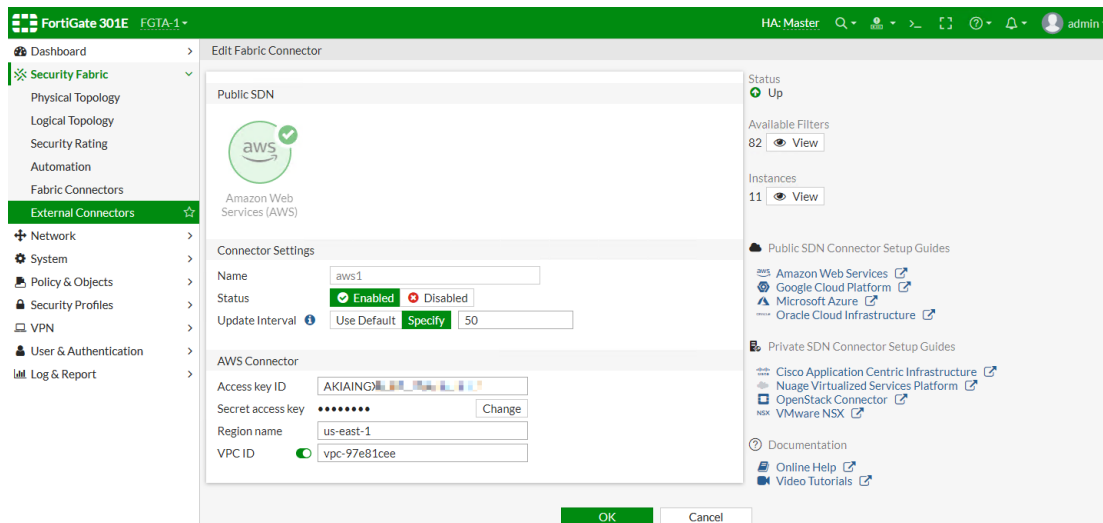
If you click *View Policies* from the tooltip, the *Fabric Connector Policies* pane shows policies that are using dynamic addresses from this Fabric connector.



If you click *View Automation Rules* from the tooltip, the *Connector Automation Rules* pane shows automation actions that are using this Fabric connector.



When you edit an existing Fabric connector, the connector status, filter, and instance information displays.



## Exchange Server connector with Kerberos KDC auto-discovery

FortiOS takes the domains learned from LDAP user authentication, and uses DNS to discover the IP addresses of Kerberos KDC servers for those domains.

The Exchange User connector is used to connect to Exchange, and other domain, servers and collect information about users. The connector can be used in conjunction with an LDAP server. The Kerberos KDC service in the domain server accepts queries to provide access and information about users in the domain.

By default, KDC discovery is automatic. If auto-discovery is disabled, the KDC IP address must be manually configured.



**To configure an Exchange connector with automatic KDC discovery:**

```

config user exchange
    edit "exchange140"
        set server-name "W2K8-SERV1"
        set domain-name "FORTINET-FSSO.COM"
        set username "Administrator"
        set password ENC XXXXXXXXXXXXXXXXXXXXXXXX
        set ip 10.1.100.140
        set auto-discover-kdc enable
    next
end

```

**To verify that auto-discovery is working:**

```

# diagnose wad debug enable category all
# diagnose wad debug enable level verbose
# diagnose debug enable
# diagnose wad user exchange test-auto-discover

wad_diag_session_acceptor(3115): diag socket 20 accepted.
_wad_fmemp_open(557): fmemp=0x12490bd8, fmemp_name='cmemp 9188 bucket', elm_sz=9188, block_
sz=73728, overhead=0, type=advanced
Starting auto-discover test for all configured user-exchanges.
[NOTE]: If any errors are returned, try manually configuring IPs for the reported errors.

wad_rpc_nspi_test_autodiscover_kdc(1835): Starting DNS SRV request for srv(0x7f938e052050)
query(_kerberos._udp.FORTINET-FSSO.COM)
wad_dns_send_srv_query(705): 1:0: sending DNS SRV request for remote peer _kerberos._
udp.FORTINET-FSSO.COM id=0
1: DNS response received for remote host _kerberos._udp.FORTINET-FSSO.COM req-id=0
wad_dns_parse_srv_resp(409): _kerberos._udp.FORTINET-FSSO.COM: resp_type(SUCCESS)
    srv[0]: name(w2k12-serv1.fortinet-fsso.com) port(88) priority(0) weight(100)
        addr[0]: 10.1.100.131
        addr[1]: 10.6.30.131
        addr[2]: 172.16.200.131
        addr[3]: 2003::131
        addr[4]: 2001::131
    srv[1]: name(fsso-core-DC.Fortinet-FSSO.COM) port(88) priority(0) weight(100)
        addr[0]: 10.6.30.16
        addr[1]: 172.16.200.16
    srv[2]: name(w2k12-serv1.Fortinet-FSSO.COM) port(88) priority(0) weight(100)
        addr[0]: 10.1.100.131
        addr[1]: 172.16.200.131
        addr[2]: 10.6.30.131
        addr[3]: 2001::131
        addr[4]: 2003::131
wad_rpc_nspi_dns_on_discover_kdc_done(1787): Received response for DNS autodiscover req
(0x7f938dfe8050) query(_kerberos._udp.FORTINET-FSSO.COM) n_rsp(3)

Completed auto-discover test for all configured user-exchanges.

```

**Support IBM Cloud SDN connector - 6.4.1**

FortiOS can automatically update dynamic addresses for IBM Cloud using an SDN connector.

The dynamic addresses can be filtered with the following filters:

- <InstanceId>
- <InstanceName>
- <ImageId>
- <ImageName>
- <Architecture>
- <Profile>
- <Vpc>
- <Zone>
- <Subnet>
- <ResourceGroup>

### To configure IBM Cloud SDN connectors using the GUI:

1. Create SDN connectors for compute generation 1 and 2:
  - a. Go to *Security Fabric > External Connectors*.
  - b. Click *Create New*, then select *IBM Cloud*.
  - c. Configure the connector for computer generation 1:

- d. Click *OK*.
- e. Click *Create New*, then select *IBM Cloud*.
- f. Configure the connector for computer generation 2:

- g. Click *OK*.
2. Create dynamic firewall addresses for the configured connectors:
  - a. Go to *Policy & Objects > Addresses*.
  - b. Click *Create New > Address*.

**c.** Configure an address for computer generation 1:

New Address

Category

Address

IPv6 Address

Multicast Address

Name

ibm\_gen1\_add1

Color

Change

Type

Dynamic

Sub Type

Fabric Connector Address

SDN Connector

ibm\_gen1

Filter

Vpc=alex-vpc1

Interface

any

Comments

Write a comment...

0/255

Dynamic Address

Guides

Configuring an AWS Dynamic Address

Configuring an Azure Dynamic Address

Configuring a Google Cloud Platform Dynamic Address

Configuring an Oracle Cloud Infrastructure Dynamic Address

Configuring an OpenStack Dynamic Address

Documentation

Online Help

Video Tutorials

- d. Click OK.
- e. Click *Create New > Address*.
- f. Configure an address for computer generation 2:

New Address

Category

Address

IPv6 Address

Multicast Address

Name

ibm\_gen2\_add1

Color

■

Change

Type

Dynamic

Sub Type

Fabric Connector Address

SDN Connector

ibm\_gen2

Filter

ResourceGroup=alex-grp2

Interface

any

Comments

Write a comment...

0/255

Dynamic Address

Guides

Configuring an AWS Dynamic Address

Configuring an Azure Dynamic Address

Configuring a Google Cloud Platform Dynamic Address

Configuring an Oracle Cloud Infrastructure Dynamic Address

Configuring an OpenStack Dynamic Address

Documentation

Online Help

Video Tutorials

- a. Click OK.
3. Ensure that the connectors resolve dynamic firewall IP addresses:
  - a. Go to *Policy & Objects* > *Addresses*.
  - b. Hover over the addresses created in step 2 to see a list of IP addresses resolved by the connector:

[illegible]

### To configure IBM Cloud SDN connectors using the CLI:

1. Create SDN connectors for compute generation 1 and 2:

```
config system sdn-connector
  edit "ibm_gen1"
    set status enable
    set type ibm
    set api-key xxxxxx
    set compute-generation 1
    set ibm-region-gen1 us-south
    set update-interval 60
  next
  edit "ibm_gen2"
    set status enable
```

```
        set type ibm
        set api-key xxxxxx
        set compute-generation 2
        set ibm-region-gen2 us-east
        set update-interval 60
    next
end
```

## 2. Create dynamic firewall addresses for the configured connectors:

```
config firewall address
    edit "ibm_gen1_add1"
        set type dynamic
        set sdn "ibm_gen1"
        set color 19
        set filter "Vpc=alex-vpc1"
    next
    edit "ibm_gen2_add1"
        set type dynamic
        set sdn "ibm_gen2"
        set color 19
        set filter "ResourceGroup=alex-grp2"
    next
end
```

## 3. Ensure that the connectors resolve dynamic firewall IP addresses:

```
# show firewall address ibm_gen1_add1
config firewall address
    edit "ibm_gen1_add1"
        set uuid 586841c4-7f46-51ea-dc66-dbf840af03d3
        set type dynamic
        set sdn "ibm_gen1"
        set color 19
        set filter "Vpc=alex-vpc1"
        config list
            edit "10.240.0.49"
            next
            edit "10.240.0.75"
            next
            edit "169.61.227.88"
            next
            edit "52.117.170.31"
            next
        end
    next
end

# show firewall address ibm_gen2_add1
config firewall address
    edit "ibm_gen2_add1"
        set uuid 5868c4f0-7f46-51ea-2b79-b5170fbfd4a8
        set type dynamic
        set sdn "ibm_gen2"
        set color 19
        set filter "ResourceGroup=alex-grp2"
        config list
            edit "10.241.128.4"
```

```

        next
        edit "10.241.128.5"
        next
        edit "10.241.129.4"
        next
        edit "52.117.126.69"
        next
    end
next
end

```

## Support ServiceTag and Region for Azure SDN connector address objects - 6.4.2

Two new filter keys, *ServiceTag* and *Region*, can be used in Azure SDN connectors to filter service tag IP ranges. These can be used in dynamic firewall addresses.

### To use the new filters keys in the GUI:

1. Create an Azure SDN connector:
  - a. Go to *Security Fabric > External Connectors* and click *Create New*.
  - b. Select *Microsoft Azure*.
  - c. Configure the connector:

- d. Click **OK**.

2. Create a dynamic firewall address for the Azure connector, filtering based on the servicetag and region:
  - a. Go to **Policy & Objects > Addresses** and click **Create New > Address**.
  - b. Configure the address, adding two filters: **ServiceTag=ApiManagement** and **Region=canadacentral**:

- c. Click **OK**.
- d. Hover the cursor over the address name to see the dynamic IP addresses that are resolved by the connector:

Name	Type	Sub Type	SDN Connector	Filter	Interface	Resolved To
azure-address-sertag1-o-region1	Dynamic	Fabric Connector Address	azure1	ServiceTag=ApiManagement   Region=canadacentral	any	102.133.0.79/32 102.133.130.197/32 102.133.154.4/31 102.133.156.0/28 102.133.26.4/31 102.133.28.0/28 104.211.146.68/31 104.211.147.144/28 104.211.81.240/28 104.211.81.28/31 104.214.18.172/31 104.214.19.224/28 104.41.217.243/32 104.41.218.160/32 13.64.39.16/32 13.66.138.92/31 13.66.140.176/28 13.67.8.108/31 13.67.9.208/28 13.69.227.76/31 13.69.229.80/28 13.69.64.76/31 13.69.66.144/28 13.70.72.240/28 13.70.72.28/31 13.71.170.44/31 13.71.172.144/28 13.71.194.116/31 13.71.196.32/28 13.71.49.1/32 13.75.217.184/32 13.75.221.78/32 13.75.34.148/31 13.75.38.16/28 13.77.50.68/31 13.77.52.224/28 13.78.106.92/31 13.78.108.176/28 13.84.189.17/32 13.85.22.63/32 13.86.102.66/32 13.87.122.84/31 13.87.123.144/28 13.87.56.84/31 13.87.57.144/28 13.89.170.204/31 13.89.174.64/28 137.117.160.56/32 191.233.203.240/28 191.233.203.28/31 191.233.24.179/32 191.233.50.192/28 191.238.241.97/32 20.150.170.224/28 20.188.77.119/32 20.192.234.160/28 20.193.202.160/28

### To use the new filters keys in the CLI:

1. Create an Azure SDN connector:

```
config system sdn-connector
  edit "azure1"
    set type azure
    set tenant-id "942b80cd-1b14-42a1-8dcf-4b21dece61ba"
    set client-id "44e79db7-621d-46f3-8625-58e209654e58"
    set client-secret xxxxxx
  next
end
```

2. Create a dynamic firewall address for the Azure connector, filtering based on the servicetag and region:

```
config firewall address
  edit "azure-address-sertag1-o-region1"
    set type dynamic
    set sdn "azure1"
    set color 2
    set filter "ServiceTag=ApiManagement | Region=canadacentral"
```

```

    next
end

```

### 3. View the dynamic IP addresses that are resolved by the connector:

```

# show firewall address azure-address-sertag1
config firewall address
    edit "azure-address-sertag1"
        set uuid 50a0afd4-b1bf-51ea-651b-f9ba7f6db455
        set type dynamic
        set sdn "azure1"
        set color 2
        set filter "ServiceTag=ApiManagement | Region=canadacentral"
    config list
        edit "102.133.0.79/32"
        next
        edit "102.133.130.197/32"
        next
        ...
        edit "13.78.108.176/28"
        next
        edit "13.86.102.66/32"
        next
        ...
    end
next
end

```

## Multiple IP addresses on Cisco ACI connectors - 6.4.4

Multiple server IP addresses can be included for the Cisco APIC cluster active and standby hosts when configuring a Cisco ACI direct SDN connector. Only one server is active, and the rest serve as backups in case the active server fails. The FortiGate checks the status of the servers, and selects one as the active server according to the order of the IP addresses in the list. If the active server fails, the FortiGate changes to the next one down on the list.

### To create an ACI direct SDN connector in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. Select *Application Centric Infrastructure (ACI)* and configure the following:

<b>Name</b>	Enter a name for the connector. In this example: <i>aci_direct1</i>
<b>Type</b>	Set to <i>Direct Connection</i> .
<b>IP</b>	Enter two IP addresses. In this example: <i>172.18.64.18</i> and <i>172.18.64.19</i>
<b>Username</b>	The ACI username.
<b>Password</b>	The ACI password.

3. Click **OK**.

### To create a dynamic address associated with the connector in the GUI:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Configure the address:

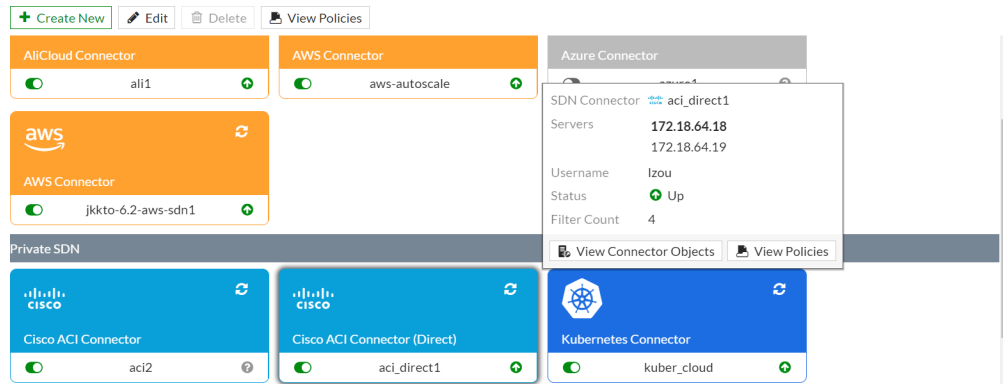
<b>Name</b>	Enter a name for the address. In this example: <i>aci_add1</i>
<b>Type</b>	<i>Dynamic</i>
<b>Sub Type</b>	<i>Fabric Connector Address</i>
<b>SDN Connector</b>	Select the just created connector: <i>aci_direct1</i>
<b>Filter</b>	Enter at least one filter. In this example: <i>Application=lzou-app</i>

3. Click **OK**.

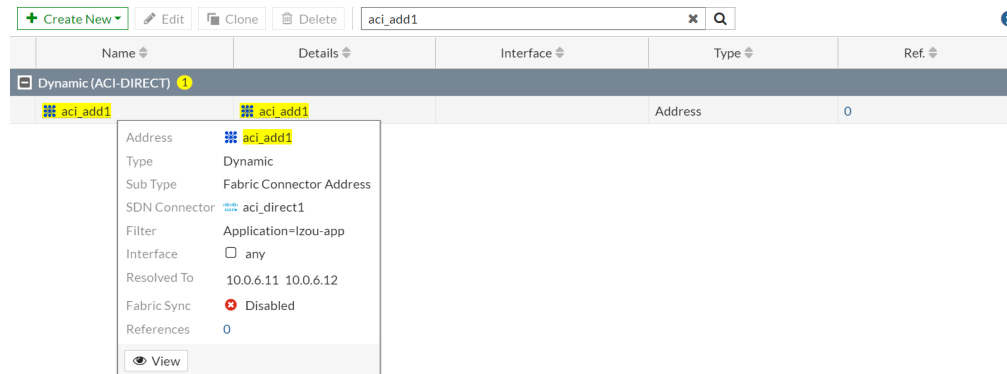


### To test that the connector is working as expected in the GUI:

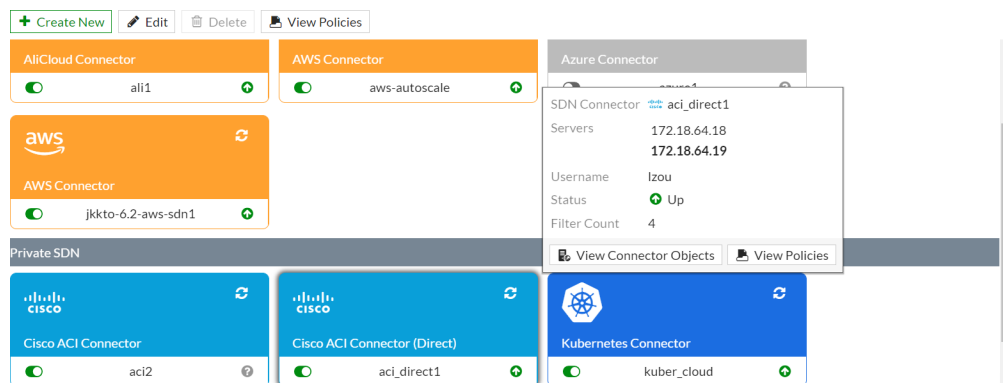
1. Go to *Security Fabric > External Connectors* and hover the cursor over the *aci\_direct1* connector to check which server is selected as the active server. The tooltip shows the IP addresses of both servers, highlighting active server in bold. In this case: **172.18.64.18**.



2. Go to *Policy & Objects > Addresses* and hover the cursor over the *aci\_add1* address. The tooltip shows the resolved addresses of the dynamic firewall address.



3. If the current active server fails, the FortiGate will choose the next server as the active server. In this case: **172.18.64.19**.



4. Recheck the resolved addresses ([Step 2](#)) to confirm that they still resolve correctly.

### To create an ACI direct SDN connector and dynamic address in the CLI:

```
config system sdn-connector
  edit "aci_direct1"
```

```
        set type aci-direct
        set server-list "172.18.64.18" "172.18.64.19"
        set username "lzou"
        set password *****
    next
end
config firewall address
    edit "aci_add1"
        set type dynamic
        set sdn "aci_direct1"
        set color 19
        set filter "Application=lzou-app"
    next
end
```

**To test that the connector is working as expected in the CLI:****1. Check which server is selected as the active server:**

```
# diagnose debug enable
# diagnose debug application acid -1
Debug messages will be on for 30 minutes.

acid sdn connector aci_direct1 updating
acid validating server status: 172.18.64.18
acid confirmed active server: 172.18.64.18
...
acid aci_direct1 sdn connector will retrieve token after 9357 secs
```

**2. Check the resolved IP addresses of the dynamic firewall address:**

```
# show firewall address aci_add1
config firewall address
    edit "aci_add1"
        set uuid c9ea564e-34d5-51eb-35e6-204876510913
        set type dynamic
        set sdn "aci_direct1"
        set color 19
        set filter "Application=lzou-app"
    config list
        edit "10.0.6.11"
        next
        edit "10.0.6.12"
        next
    end
next
end
```

**3. If the current active server fails, the FortiGate will choose the next server as the active server:**

```
# diagnose debug enable
# diagnose debug application acid -1
Debug messages will be on for 30 minutes.

acid sdn connector aci_direct1 updating
acid validating server status: 172.18.64.18
acid curl failed, 7
acid server 172.18.64.18 is down
```

```

acid validating server status: 172.18.64.19
acid confirmed active server: 172.18.64.19
...
acid aci_direct1 sdn connector will retrieve token after 8259 secs

```

4. Recheck the resolved addresses to confirm that they still resolve correctly.

## Multiple clusters on Cisco ACI connectors - 6.4.9

Multiple ACI clusters used in HA can be included for external Cisco ACI SDN connector VMs. When creating a Cisco ACI SDN connector, configuring multiple IPs allows the FortiGate to connect to SDN connector VMs in the same ACI cluster in a round-robin fashion. Only one SDN connector VM is active, and the remaining serve as backups if the active one fails.

In this example, two Cisco ACI cluster SDN connectors are configured (`aci_robot_238` and `aci_robot_239`). Each cluster contains two Cisco ACI SDN connector VMs.

### To create ACI cluster SDN connectors in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. Select *Application Centric Infrastructure (ACI)* and configure the following:

<b>Name</b>	<code>aci_robot_238</code>
<b>Type</b>	Set to <i>FortiSDN Connector</i> .
<b>IP</b>	Enter two IP addresses: <code>10.6.30.38</code> and <code>10.6.30.238</code> .
<b>Port</b>	Set to <i>Specify</i> and enter <code>5671</code> .
<b>Username</b>	Enter the ACI username.
<b>Password</b>	Enter the ACI password.

**Edit External Connector**

**Private SDN**

Application Centric Infrastructure (ACI)

**Connector Settings**

Name: `aci_robot_238`

Status: ☒ Enabled ☐ Disabled

**Cisco ACI Connector**

Type: **FortiSDN Connector** Direct Connection

IP: `10.6.30.38` `10.6.30.238`

Port: Use Default **Specify** `5671`

Username: `admin`

Password: `*****`

Status: ☒ Up

**Public SDN Connector Setup Guides**

- [Amazon Web Services](#)
- [Google Cloud Platform](#)
- [Microsoft Azure](#)
- [Oracle Cloud Infrastructure](#)

**Private SDN Connector Setup Guides**

- [Cisco Application Centric Infrastructure](#)
- [Nuage Virtualized Services Platform](#)
- [OpenStack Connector](#)
- [VMware NSX](#)

**Documentation**

- [Online Help](#)
- [Video Tutorials](#)

- Click *OK*.
- Repeat these steps to create another connector with the following settings:

<b>Name</b>	<i>aci_robot_239</i>
<b>Type</b>	Set to <i>FortiSDN Connector</i> .
<b>IP</b>	Enter two IP addresses: <i>10.6.30.39</i> and <i>10.6.30.239</i> .
<b>Port</b>	Set to <i>Specify</i> and enter <i>5671</i> .
<b>Username</b>	Enter the ACI username.
<b>Password</b>	Enter the ACI password.

### To create dynamic addresses associated with the connectors in the GUI:

- Go to *Policy & Objects > Addresses* and click *Create New > Address*.
- Configure the following:

<b>Name</b>	<i>aci-add-App-238</i>
<b>Type</b>	<i>Dynamic</i>
<b>Sub Type</b>	<i>Fabric Connector Address</i>
<b>SDN Connector</b>	<i>aci_robot_238</i>
<b>Tenant</b>	<i>Fortinet</i>
<b>Endpoint Group Name</b>	<i>App1</i>

The screenshot shows the 'Edit Address' configuration window in the FortiGate GUI. The 'Category' is set to 'Address'. The 'Name' field contains 'aci-add-App-238'. The 'Type' is set to 'Dynamic'. The 'Sub Type' is set to 'Fabric Connector Address'. The 'SDN Connector' is set to 'aci\_robot\_238'. The 'Tenant' is set to 'Fortinet'. The 'Endpoint Group Name' is set to 'App1'. The 'Interface' is set to 'any'. The 'Comments' field is empty. The 'OK' button is highlighted in green.

- Click *OK*.
- Repeat these steps to create another dynamic address with the following settings:

<b>Name</b>	<i>aci-add-App-239</i>
<b>Type</b>	<i>Dynamic</i>
<b>Sub Type</b>	<i>Fabric Connector Address</i>
<b>SDN Connector</b>	<i>aci_robot_239</i>
<b>Tenant</b>	<i>Fortinet</i>
<b>Endpoint Group Name</b>	<i>App1</i>

**To test that firewall addresses can resolve the dynamic addresses based on the SDN connector in the GUI:**

1. Go to *Policy & Objects > Addresses*.
2. Hover the cursor over an address. The tooltip shows the resolved addresses of the dynamic firewall address.

The screenshot shows the FortiGate GUI's 'Addresses' section. At the top, there are buttons for 'Create New', 'Edit', 'Clone', 'Delete', and a search bar. A 'Synchronized' status indicator is on the right. Below is a table with columns: Name, Details, Interface, Fabric Sync, Type, and Ref. Two dynamic addresses are listed: 'aci-add-App-238' and 'aci-add-App-239'. A tooltip is open for 'aci-add-App-239', displaying its configuration: Address (aci-add-App-239), Type (Dynamic), Sub Type (Fabric Connector Address), SDN Connector (aci\_robot\_239), Tenant (Fortinet), Endpoint Group Name (App1), Interface (any), and a list of resolved IP addresses. The Fabric Sync status is 'Disabled' and there are 0 references. An 'Edit' button is at the bottom of the tooltip. At the bottom right of the GUI, it shows '2/75' and 'Updated: 11:06:39'.

Name	Details	Interface	Fabric Sync	Type	Ref.
aci-add-App-238	aci-add-App-238		Disable	Address	0
aci-add-App-239	aci-add-App-239		Disable	Address	0

Address: aci-add-App-239

Type: Dynamic

Sub Type: Fabric Connector Address

SDN Connector: aci\_robot\_239

Tenant: Fortinet

Endpoint Group Name: App1

Interface: any

Resolved To:

57.244.141.1	42.204.249.3	113.20.146.15
222.20.244.24	136.111.120.28	232.68.132.53
159.10.165.63	158.68.111.87	193.182.254.90
153.11.53.97	137.225.232.98	127.139.171.102
246.238.232.107	189.130.189.117	145.225.9.121
61.85.89.127	254.63.148.141	255.101.230.147
164.95.140.151	118.223.37.174	213.112.26.175
67.82.175.177	171.90.109.180	15.216.40.190
106.97.0.201	247.186.79.208	112.237.77.209
21.90.161.213	156.8.243.247	79.85.64.251

Fabric Sync: Disabled

References: 0

**To create ACI cluster SDN connectors in the CLI:**

```
config system sdn-connector
  edit "aci_robot_238"
    set type aci
    set server-list "10.6.30.38" "10.6.30.238"
    set server-port 5671
    set username "admin"
    set password *****
  next
  edit "aci_robot_239"
    set type aci
    set server-list "10.6.30.39" "10.6.30.239"
    set server-port 5671
    set username "admin"
    set password *****
  next
end
```

**To create dynamic addresses associated with the connectors in the CLI:**

```
config firewall address
  edit "aci-add-App-238"
    set type dynamic
    set sdn "aci_robot_238"
    set color 17
    set tenant "Fortinet"
```

```
        set epg-name "App1"
    next
    edit "aci-add-App-239"
        set type dynamic
        set sdn "aci_robot_239"
        set color 17
        set tenant "Fortinet"
        set epg-name "App1"
    next
end
```

**To test that firewall addresses can resolve the dynamic addresses based on the SDN connector in the CLI:**

**1. Check the aci-add-App-238 address:**

```
# diagnose firewall dynamic address aci-add-App-238
aci_robot_238.aci.Fortinet.App1.*: ID(90)
    ADDR(244.141.232.3)
    ADDR(124.37.216.5)
    ADDR(178.77.227.6)
    ...
    ADDR(87.26.255.252)
    ADDR(31.45.199.254)
    ADDR(154.149.224.254)

Total dynamic list entries: 1.
Total dynamic addresses: 150
Total dynamic ranges: 0
```

**2. Check the aci-add-App-239 address:**

```
# diagnose firewall dynamic address aci-add-App-239
aci_robot_239.aci.Fortinet.App1.*: ID(91)
    ADDR(57.244.141.1)
    ADDR(42.204.249.3)
    ADDR(113.20.146.15)
    ...
    ADDR(21.90.161.213)
    ADDR(156.8.243.247)
    ADDR(79.85.64.251)

Total dynamic list entries: 1.
Total dynamic addresses: 30
Total dynamic ranges: 0
```

## Update OpenStack SDN connector to support the latest OpenStack releases - 6.4.9

Updating dynamic addresses using the OpenStack SDN connector now supports: Rocky, Stein, Train, Ussuri, Victoria, Wallaby, and Xena.

In this example, two OpenStack SDN connectors are configured (OpenStackWallaby and OpenStackXena).

**To configure the OpenStack SDN connectors in the GUI:**

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. Select *OpenStack (Horizon)* and configure the following:

<b>Name</b>	<i>OpenStackWallaby</i>
<b>Verify certificate</b>	Disable
<b>Server</b>	Enter the IP address: <i>34.145.74.207</i> .
<b>Username</b>	Enter the OpenStack username.
<b>Password</b>	Enter the OpenStack password.
<b>Domain</b>	Enter the OpenStack domain.

3. Click *OK*.
4. Repeat these steps to create another connector with the following settings:

<b>Name</b>	<i>OpenStackXena</i>
<b>Verify certificate</b>	Disable
<b>Server</b>	Enter the IP address: <i>35.197.67.163</i> .
<b>Username</b>	Enter the OpenStack username.
<b>Password</b>	Enter the OpenStack password.
<b>Domain</b>	Enter the OpenStack domain.

**To configure the OpenStack SDN connectors in the CLI:**

```
config system sdn-connector
  edit "OpenStackWallaby"
    set type openstack
    set verify-certificate disable
    set server "34.145.74.207"
    set username "admin"
    set password *****
    set domain "E2-*****-ZTNA_HoL_v1.0-*****"
  next
  edit "OpenStackXena"
    set type openstack
    set verify-certificate disable
    set server "35.197.67.163"
    set username "admin"
    set password *****
    set domain "E2-*****-ZTNA_HoL_v1.0-*****"
  next
end
```

**To configure dynamic addresses associated with the connectors in the GUI:**

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Configure the following:

<b>Name</b>	<i>WallabyAddress</i>
<b>Type</b>	<i>Dynamic</i>
<b>Sub Type</b>	<i>Fabric Connector Address</i>
<b>SDN Connector</b>	<i>OpenStackWallaby</i>
<b>SDN address type</b>	<i>All</i>
<b>Filter</b>	<i>Name=testvm4</i>

3. Click **OK**.
4. Repeat these steps to create another dynamic address with the following settings:

<b>Name</b>	<i>XenaAddress</i>
<b>Type</b>	<i>Dynamic</i>
<b>Sub Type</b>	<i>Fabric Connector Address</i>
<b>SDN Connector</b>	<i>OpenStackXena</i>
<b>SDN address type</b>	<i>All</i>
<b>Filter</b>	<i>Name=testvm3</i>

#### To configure dynamic addresses associated with the connectors in the CLI:

```
config firewall address
  edit "WallabyAddress"
    set type dynamic
    set sdn "OpenStackWallaby"
    set filter "Name=testvm4"
    set sdn-addr-type all
  next
  edit "XenaAddress"
    set type dynamic
    set sdn "OpenStackXena"
    set filter "Name=testvm3"
    set sdn-addr-type all
  next
end
```

#### To test that firewall addresses can resolve the dynamic addresses based on the SDN connector in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Hover the cursor over the address name.



Name	Details	Interface	Type	Ref.
IP Range/Subnet				
FABRIC			Address	0
FIREW			Address	0
SSLVP		10.212.134.210	Address	2
all			Address	0
none			Address	0
FortiClient				
FCEN			Address	0
Dynamic (C				
Wallab			Address	0
XenaAddress			Address	0

The tooltip shows the resolved addresses of the dynamic firewall address.

**To test that firewall addresses can resolve the dynamic addresses based on the SDN connector in the CLI:**

```
# show firewall address
config firewall address
  edit "WallabyAddress"
    set uuid e42d9e80-bba2-51ec-9d14-2e85213c4b8f
    set type dynamic
    set sdn "OpenStackWallaby"
    set filter "Name=testvm4"
    set sdn-addr-type all
  config list
    edit "10.0.0.118"
    next
    edit "172.24.4.247"
    next
  end
next
edit "XenaAddress"
  set uuid 34b89196-bba5-51ec-30c0-1a12c98806c5
  set type dynamic
  set sdn "OpenStackXena"
  set filter "Name=testvm3"
  set sdn-addr-type all
  config list
    edit "10.0.0.232"
    next
    edit "172.24.4.77"
    next
  end
next
end
```

## Automation stitches

This section includes information about automation stitches related new features:

- [Automation stitches on page 100](#)
- [Slack notification action on page 109](#)
- [NSX-T quarantine action 6.4.1 on page 113](#)
- [FortiNAC quarantine action for automation 6.4.2 on page 116](#)

## Automation stitches

Eight new webhook automation stitches were added to the *Automation* menu. The additional stitches include a new *Incoming Webhook Quarantine* trigger for API calls to the FortiGate, as well as a predefined *License Expired Notification* that replaces the existing license expiry alerts.

The automation stitches are available in new FortiGate installations by default. To install the stitches on an existing device, perform a factory reset.



Performing a factory reset will wipe the existing configurations from the FortiGate. Before performing a factory reset, backup the existing configuration. Contact Fortinet support for additional assistance.

The following webhook stitches were added to the *Automation* menu:

- Compromised Host Quarantine
- Incoming Webhook quarantine
- HA Failover
- Network Down
- Reboot
- FortiAnalyzer Connection Down
- License Expired Notification
- Security rating Notification

## GUI

To view the new automation stitches in the GUI, go to *Security Fabric > Automation*.

Name	Trigger	Status	Last Trigger Time
Access Layer Quarantine			
Quarantine FortiClient via EMS			
Compromised Host Quarantine	Compromised Host	Disabled	
Incoming Webhook Quarantine	Incoming Webhook	Disabled	
Email			
HA Failover	HA Failover	Disabled	
Network Down	FortiOS Event Log	Disabled	
Reboot	Reboot	Disabled	
FortiExplorer Notification			
FortiAnalyzer Connection Down	FortiOS Event Log	Enabled	
License Expired Notification	License Expiry	Enabled	
Security Rating Notification	Security Rating Summary	Enabled	



After the factory reset, the email alert feature will be removed from the GUI (*Log & Report > Email Alert Settings*), and replaced with the *Email* automation stitches. You can continue using the email alert feature with the CLI console.

## CLI

To configure the new automation stitches in the CLI console, use the following commands:

```
config system automation-action
config system automation-trigger
config system automation-stitch
```

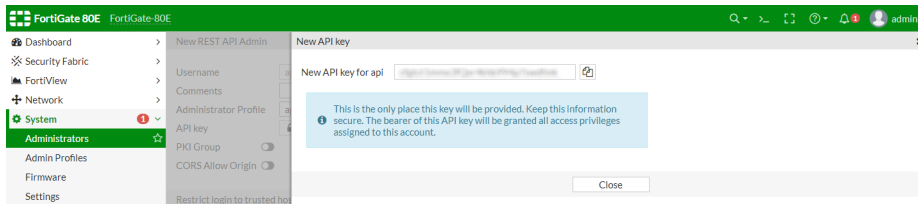


To view the configurations for the new automation stitches, see the CLI reference at the bottom of the page.

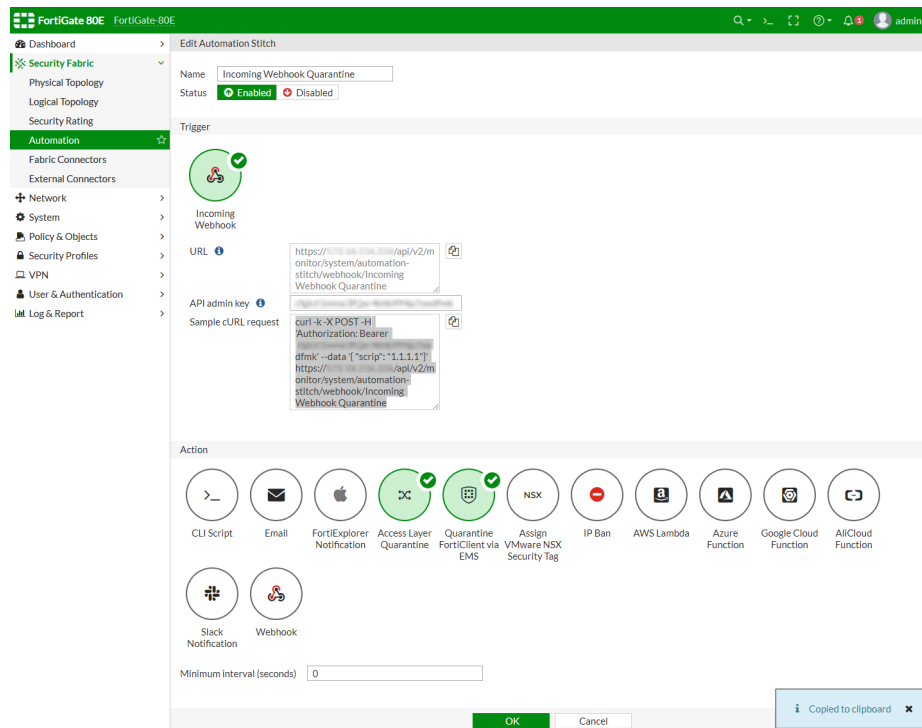
---

## To trigger an Incoming Webhook Quarantine stitch with the GUI:

1. Create new API user.
  - a. Go to *System > Administrators*.
  - b. Click *Create New > REST API Admin*.
  - c. Configure the *New REST API Admin* settings, and record the API key.



2. Get the sample cURL request.
  - a. Go to *Security Fabric > Automation*.
  - b. Under *Incoming Webhook*, right-click *Incoming Webhook Quarantine*, and select *Edit*.
  - c. Click *Enabled*, to enable the rule.
  - d. In the *API admin key* field, enter the API key you recorded in the previous step. A *Sample cURL request* is created.
  - e. Copy the *Sample cURL request*.



### 3. Execute the request:

a. Edit the sample cURL you recorded in the previous step.

b. Add parameters to the data field ("mac" and "fctuid"), and then execute the request.

```
root@pc:~# curl -k -X POST -H 'Authorization: Bearer
cfgtctlmmx3fQxr4kxb994p7swdfmk' --data '{ "mac": "0c:0a:00:0c:ce:b0", "fctuid":
"0000BB0B0ABD0D00B0D0A0B0E0F0B00B"}'
https://172.16.116.226/api/v2/monitor/system/automation-
stitch/webhook/Incoming%20Webhook%20Quarantine
{
  "http_method": "POST",
  "status": "success",
  "http_status": 200,
  "serial": "FGT00E0Q00000000",
  "version": "v6.4.0",
  "build": 1545
}
```



Encode the spaces in the automation-stitch name with %20. For example,  
Incoming%20Webhook%20Quarantine

The automation rule *Incoming Webhook Quarantine* is triggered.

Name	Trigger	Status	Last Trigger Time
Access Layer Quarantine	Quarantine FortiClient via EMS		
Compromised Host Quarantine	Compromised Host	Disabled	
Incoming Webhook Quarantine	Incoming Webhook	Enabled	2020/02/14 15:37:48
Email			
HA Failover	HA Failover	Disabled	
Network Down	FortiOS Event Log	Disabled	
Reboot	Reboot	Disabled	
FortiExplorer Notification			
FortiAnalyzer Connection Down	FortiOS Event Log	Enabled	
License Expiry Notification	License Expiry	Enabled	
Security Rating Notification	Security Rating Summary	Enabled	

The MAC address is quarantined in FortiGate and an event log is created.

The FortiClient UUID is quarantined by EMS on the server side.

Date/Time	Level	User	Message
2020/02/14 15:37:48	Info	auto-join	stitch:incoming Webhook Quarantine is triggered.
2020/02/14 15:37:25	Info	auto-join	FortiCloud service activation failed
2020/02/14 15:37:25	Info	auto-join	Attempted to join FortiCloud
2020/02/14 15:35:52	Info		Performance statistics: average CPU: 4, memory: 30, concurrent sess
2020/02/14 15:35:28	Info		Pid: 02573, application: forticron, Firmware: FortiGate-80E v6.4.0.bx
2020/02/14 15:30:28	Info		Performance statistics: average CPU: 0, memory: 30, concurrent sess
2020/02/14 15:27:25	Info	auto-join	FortiCloud service activation failed
2020/02/14 15:27:25	Info	auto-join	Attempted to join FortiCloud
2020/02/14 15:25:28	Info		Performance statistics: average CPU: 4, memory: 30, concurrent sess
2020/02/14 15:25:03	Info		Pid: 02493, application: forticron, Firmware: FortiGate-80E v6.4.0.bx
2020/02/14 15:20:55	Info	admin	Edit system.automation-stitch Security Rating Notification
2020/02/14 15:20:52	Info	admin	Edit system.automation-stitch Security Rating Notification
2020/02/14 15:20:22	Info	admin	Edit system.automation-stitch Incoming Webhook Quarantine
2020/02/14 15:20:19	Info	admin	Rename system.automation-trigger Incoming Webhook Call to Incon
2020/02/14 15:20:04	Info		Performance statistics: average CPU: 0, memory: 30, concurrent sess
2020/02/14 15:17:25	Info	auto-join	FortiCloud service activation failed
2020/02/14 15:17:25	Info	auto-join	Attempted to join FortiCloud
2020/02/14 15:14:39	Info		Performance statistics: average CPU: 4, memory: 30, concurrent sess
2020/02/14 15:14:01	Info		Pid: 02413, application: forticron, Firmware: FortiGate-80E v6.4.0.bx

**Log Details**  
 Date: 2020/02/14  
 Time: 15:37:48  
 Virtual Domain: root  
 Log Description: Automation stitch triggered  
 Source: User  
 Action: Action undefined  
 Security: Event  
 From: log  
 Message: stitch:incoming Webhook Quarantine is triggered.  
 Other:  
 Log ID: 0100046600  
 Type: event  
 Sub Type: system  
 Log event: original  
 timestamp: 1581723468644200700  
 Timezone: -0800  
 Stitch: Incoming Webhook Quarantine  
 Trigger: Incoming Webhook Quarantine  
 Action: Quarantine\_quarantine,Compromised Host Quarantine\_quarantine-forticlient

## To create an automated stitch with the CLI:

### 1. Create new API user and record the API key.

```
config system api-user
  edit "api"
    set api-key ENC SH00vqP0GKWKyZNz0FP0/jq0000Ka/DHVEKdxUi+0kRDNKPpZppnnMk0KeunBI=
    set accprofile "api_profile"
    set vdom "root"
  config trusthost
    edit 1
      set ipv4-trusthost 10.6.30.0 200.200.200.0
    next
  end
next
end
```

### 2. Configure the automation stitch, Incoming Webhook Quarantine.

```
config system automation-stitch
  edit "Incoming Webhook Quarantine"
    set status enable
    set trigger "Incoming Webhook Quarantine"
    set action "Compromised Host Quarantine_quarantine" "Compromised Host Quarantine_quarantine-forticlient"
  next
end
```

**3. Add parameters in the data field ("mac" and "fctuid"), then execute the request on a device.**

```
root@pc56:~# curl -k -X POST -H 'Authorization: Bearer
cftgtctlmmx0fQxr4kxb000p70wdfmk' --data '{ "mac": "0c:0a:00:0c:ce:b0", "fctuid":
"3000BB0B0ABD0D00B0D0A0B0E0F0B00B"}'
https://100.10.100.200/api/v2/monitor/system/automation-
stitch/webhook/Incoming%20Webhook%20Quarantine
{
  "http_method": "POST",
  "status": "success",
  "http_status": 200,
  "serial": "FGT80E0Q000000000",
  "version": "v6.4.0",
  "build": 1545
}
```



Encode the spaces in the automation-stitch name with %20. For example,  
Incoming%20Webhook%20Quarantine

The automation rule "Incoming Webhook Quarantine" is triggered. The MAC address is quarantined in FortiGate, and an event log is created. The FortiClient UUID will be quarantined on the EMS server side.

```
config user quarantine
  config targets
    edit "0c:0a:00:0c:ce:b0"
      config macs
        edit 0c:0a:00:0c:ce:b0
          set description "Quarantined by automation stitch: Incoming Webhook
            Quarantine"
        next
      end
    next
  end
end
date=2020-02-14 time=15:37:48 logid="0100046600" type="event" subtype="system"
level="notice" vd="root" eventtime=1581723468644200712 tz="-0800"
logdesc="Automation stitch triggered" stitch="Incoming Webhook Quarantine"
trigger="Incoming Webhook Quarantine" stitchaction="Compromised Host Quarantine_
quarantine,Compromised Host Quarantine_quarantine-forticlient" from="log"
msg="stitch:Incoming Webhook Quarantine is triggered."
```

## CLI Reference

### Network down

#### config system automation-action

```
config system automation-action
  edit "Network Down_email"
    set action-type email
    set email-from ''
    set email-subject "Network Down"
    set minimum-interval 0
    set delay 0
```

```
        set required disable
        set message "%log%"
    next
end
```

### **config system automation-trigger**

```
config system automation-trigger
    edit "Network Down"
        set trigger-type event-based
        set event-type event-log
        set logid 20099
        config fields
            edit 1
                set name "status"
                set value "DOWN"
            next
        end
    next
end
```

### **config system automation-stitch**

```
config system automation-stitch
    edit "Network Down"
        set status disable
        set trigger "Network Down"
        set action "Network Down_email"
    next
end
```

## **HA failover**

### **config system automation-action**

```
config system automation-action
    edit "HA Failover_email"
        set action-type email
        set email-from ''
        set email-subject "HA Failover"
        set minimum-interval 0
        set delay 0
        set required disable
        set message "%log%"
    next
end
```

### **config system automation-trigger**

```
config system automation-trigger
    edit "HA Failover"
        set trigger-type event-based
        set event-type ha-failover
    next
end
```

**config system automation-stitch**

```
config system automation-stitch
  edit "HA Failover"
    set status disable
    set trigger "HA Failover"
    set action "HA Failover_email"
  next
end
```

**Reboot****config system automation-action**

```
config system automation-action
  edit "Reboot_email"
    set action-type email
    set email-from ''
    set email-subject "Reboot"
    set minimum-interval 0
    set delay 0
    set required disable
    set message "%log%"
  next
end
```

**config system automation-trigger**

```
config system automation-trigger
  edit "Reboot"
    set trigger-type event-based
    set event-type reboot
  next
end
```

**config system automation-stitch**

```
config system automation-stitch
  edit "Reboot"
    set status disable
    set trigger "Reboot"
    set action "Reboot_email"
  next
end
```

**Connection down****config system automation-action**

```
config system automation-action
  edit "FortiAnalyzer Connection Down_ios-notification"
    set action-type ios-notification
    set minimum-interval 0
    set delay 0
    set required disable
```



```
    next
end
```

### **config system automation-trigger**

```
config system automation-trigger
    edit "FortiAnalyzer Connection Down"
        set trigger-type event-based
        set event-type event-log
        set logid 22902
    next
end
```

### **config system automation-stitch**

```
config system automation-stitch
    edit "FortiAnalyzer Connection Down"
        set status enable
        set trigger "FortiAnalyzer Connection Down"
        set action "FortiAnalyzer Connection Down_ios-notification"
    next
end
```

## **License expired**

### **config system automation-action**

```
config system automation-action
    edit "License Expired Notification_ios-notification"
        set action-type ios-notification
        set minimum-interval 0
        set delay 0
        set required disable
    next
end
```

### **config system automation-trigger**

```
config system automation-trigger
    edit "License Expired Notification"
        set trigger-type event-based
        set event-type license-near-expiry
        set license-type any
    next
end
```

### **config system automation-stitch**

```
config system automation-stitch
    edit "License Expired Notification"
        set status enable
        set trigger "License Expired Notification"
        set action "License Expired Notification_ios-notification"
    next
end
```

## Compromised host

### config system automation-action

```
config system automation-action
  edit "Compromised Host Quarantine_quarantine"
    set action-type quarantine
    set minimum-interval 0
    set delay 0
    set required disable
  next
end
```

### config system automation-trigger

```
config system automation-trigger
  edit "Compromised Host Quarantine"
    set trigger-type event-based
    set event-type ioc
    set ioc-level high
  next
end
```

### config system automation-stitch

```
config system automation-stitch
  edit "Compromised Host Quarantine"
    set status disable
    set trigger "Compromised Host Quarantine"
    set action "Compromised Host Quarantine_quarantine" "Compromised Host Quarantine_
      quarantine-forticlient"
  next
end
```

## Quarantine FortiClient

### config system automation-action

```
config system automation-action
  edit "Compromised Host Quarantine_quarantine-forticlient"
    set action-type quarantine-forticlient
    set minimum-interval 0
    set delay 0
    set required disable
  next
end
```

### config system automation-trigger

```
config system automation-trigger
  edit "Compromised Host Quarantine"
    set trigger-type event-based
    set event-type ioc
    set ioc-level high
  next
```

```
end
```

### **config system automation-stitch**

```
config system automation-stitch
  edit "Compromised Host Quarantine"
    set status disable
    set trigger "Compromised Host Quarantine"
    set action "Compromised Host Quarantine_quarantine" "Compromised Host Quarantine_
      quarantine-forticlient"
  next
end
```

## **Security rating**

### **config system automation-action**

```
config system automation-action
  edit "Security Rating Notification_ios-notification"
    set action-type ios-notification
    set minimum-interval 0
    set delay 0
    set required disable
  next
end
```

### **config system automation-trigger**

```
config system automation-trigger
  edit "Security Rating Notification"
    set trigger-type event-based
    set event-type security-rating-summary
  next
end
```

### **config system automation-stitch**

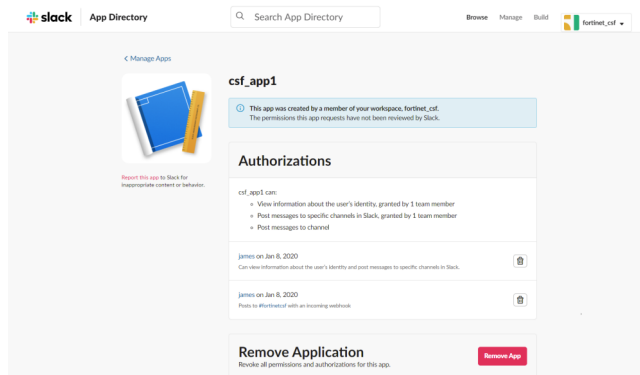
```
config system automation-stitch
  edit "Security Rating Notification"
    set status enable
    set trigger "Security Rating Notification"
    set action "Security Rating Notification_ios-notification"
  next
end
```

## **Slack notification action**

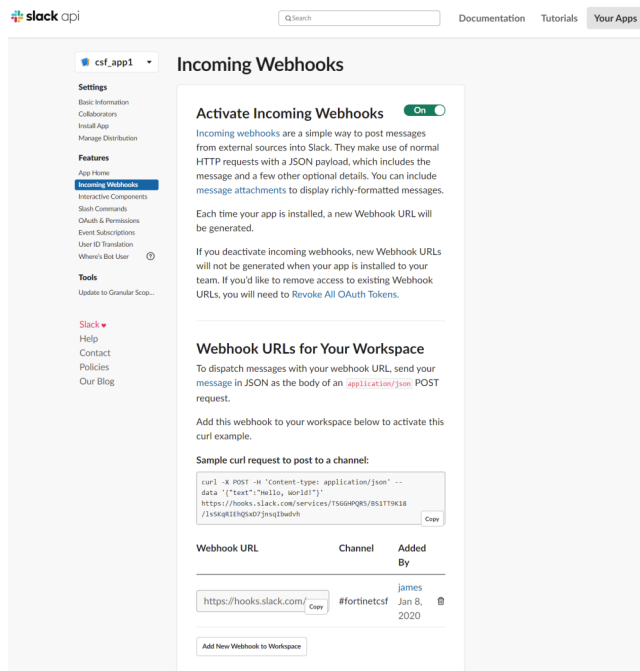
Automation stitches now include a Slack notification in the *Action* menu. To configure the automation stitch, create an Incoming Webhook in Slack, and then enter the Webhook URL in the corresponding field of the notification action in FortiGate.

## To create an Incoming Webhook in Slack:

1. Go to the Slack website, and create a workspace.
2. Create a Slack application for the workspace.



3. Add an *Incoming Webhook* to a channel in the workspace.
4. Activate the *Incoming Webhook*, and record the *Webhook URL*.



For information about using Incoming Webhooks in Slack, see <https://api.slack.com/incoming-webhooks>.

## To configure a Slack notification in the GUI:

1. Go to *Security Fabric > Automation*.
2. Choose an automation stitch, and click *Edit*.

### 3. Select *Slack Notification*, and configure the notification settings.

The screenshot shows the FortiGate VM64 Security Fabric Automation configuration interface. The 'Automation' section is selected in the left sidebar. The 'Edit Automation Stitch' window is open, showing a trigger for 'Security Rating Summary' and an action for 'Slack Notification'. The 'Slack Notification' configuration includes two actions: 'slack1' and 'slack2'. 'slack1' has a delay of 0 seconds and a message 'This is test for slack notification.' 'slack2' has a delay of 90 seconds and a message '%log%'. The 'URL' for both actions is 'https://hooks.slack.com/services/TSGGHPQR5/BS1TT9K18/lSKqRIEhQsxD7jnsqIbwdvh'.

<b>Name</b>	Enter a name for the notification.
<b>Delay</b>	Enter the number of seconds to delay the notification after the previous action is triggered.
<b>URL</b>	Enter the <i>Webhook URL</i> you recorded when you created the Incoming Webhook in Slack.
<b>Message</b>	<p>Take one of the following actions:</p> <ul style="list-style-type: none"> <li>Configure the message parameters. Click % to view a description of the available parameters.</li> <li>Enter the message to display in the Slack channel.</li> </ul>

#### 4. (Optional) Click the plus (+) sign to add another action.

#### 5. Click OK.

#### 6. Run the automation stitch to trigger the action.

### To configure a Slack notification in the CLI:

#### 1. Add the webhook URL the Slack notification action.

```
config system automation-action
edit "slack1"
set action-type slack-notification
set minimum-interval 0
set delay 0
set required disable
set message "This is test for slack notification."
set uri "hooks.slack.com/services/TSGGHPQR5/BS1TT9K18/lSKqRIEhQsxD7jnsqIbwdvh"
next
edit "slack2"
set action-type slack-notification
```

```

set minimum-interval 0
set delay 90
set required disable
set message "%log%"
set uri "hooks.slack.com/services/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"
next
end

```

## 2. Create the trigger for the notification.

```

config system automation-trigger
edit "auto-rating"
set trigger-type event-based
set event-type security-rating-summary
next
end

```

## 3. Configure the action for the trigger.

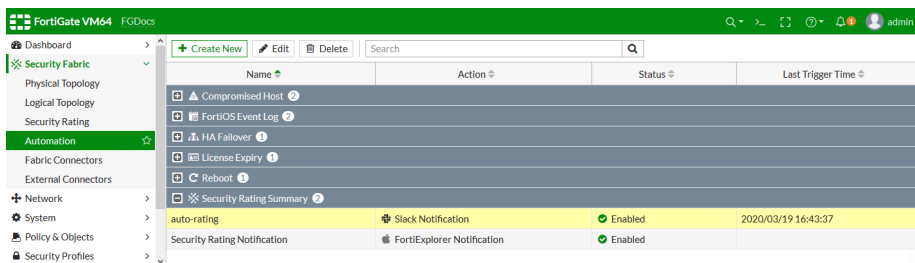
```

config system automation-stitch
edit "auto-rating"
set status enable
set trigger "auto-rating"
set action "slack1" "slack2"
next
end

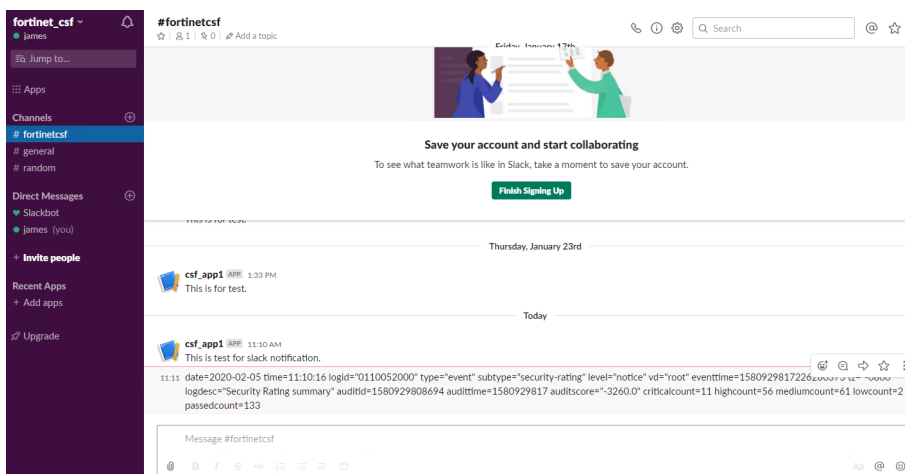
```

## 4. Trigger the notification.

The notification action is triggered in FortiGate.



The message you entered in the automation stitch is delivered to the Slack channel.



## NSX-T quarantine action - 6.4.1

New CLI options have been added for VMware NSX SDN connectors to configure the vCenter server and credentials so the FortiGate can resolve NSX-T VMs.

The FortiGate is notified of a compromised host on the NSX-T network by an incoming webhook or other means, such as FortiGuard IOC. An automation stitch can be configured to process this trigger and action it by assigning a VMware NSX security tag on the VM instance.

### To configure an automation stitch to assign a security tag to NSX-T VMs in the GUI:

#### 1. Configure the NSX SDN connector:

```
config system sdn-connector
  edit "nsx_t25"
    set type nsx
    set server "172.18.64.205"
    set username "admin"
    set password xxxxxx
    set vcenter-server "172.18.64.201"
    set vcenter-username "administrator@vsphere.local"
    set vcenter-password xxxxxx
  next
end
```

#### 2. Configure the automation stitch:

- a. Go to *Security Fabric > Automation* and click *Create New*.
- b. In the *Trigger* section, select *Incoming Webhook*.
- c. In the *Action* section, select *Assign VMwareNSX Security Tag*.
- d. Enable *Specify NSX server(s)* and enter a server.
- e. Enter a *Security tag*.

## f. Click OK.


Edit Automation Stitch

Name: auto\_webhook

Status: ● Enabled ● Disabled

FortiGate: All FortiGates

Trigger

 Incoming Webhook

URL: [https://172.16.116.230/api/v2/monitor/system/automation-stitch/webhook/auto\\_webhook](https://172.16.116.230/api/v2/monitor/system/automation-stitch/webhook/auto_webhook)

API admin key:

Sample cURL request: 

```
curl -k -X POST -H 'Authorization: Bearer <API key>' --data '{
  "srcip": "1.1.1.1",
  "mac": "11-11-11-11-11-11",
  "cloud": "ASB8ADB12DA694E47BA4ADF24F836B62F"
}' https://172.16.116.230/api/v2/monitor/system/automation-stitch/webhook/auto_webhook...
```

Action

☒ CLI Script
 ☐ Email
 ☐ FortiExplorer Quarantine
 ☐ Access Layer Quarantine
 ☐ Quarantine FortiClient
 ☒ Assign VMware NSX Security Tag
 ☐ IP Ban
 ☐ AWS Lambda
 ☐ Azure Function
 ☐ Google Cloud Function

☐ AWS Cloud Function
 ☐ Slack Notification
 ☐ Webhook

Minimum interval (seconds):

Assign VMware NSX Security Tag

Specify NSX server(s): ☒ nsx\_t25

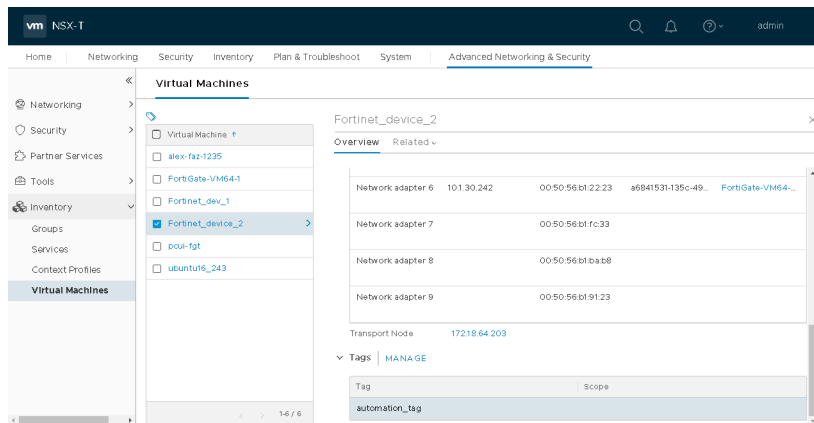
Security tag:

## 3. In NSX-T, create a cURL request to trigger the automation stitch on the FortiGate:

```
root@pc56:/home# curl -k -X POST -H 'Authorization: Bearer
3fdxNG08mgNg0fh4NQ51g1NQ1QHcxx' --data '{ "srcip": "10.1.30.242"}'
https://172.16.116.230/api/v2/monitor/system/automation-stitch/webhook/auto_webhook
{
  "http_method": "POST",
  "status": "success",
  "http_status": 200,
  "serial": "FGVM08TM20000220",
  "version": "v6.4.0",
  "build": 1608
}
```

The automation stitch is triggered and the configured tag is added to the NSX-T VM.





In FortiOS, the *Security Fabric > Automation* page shows the last trigger time.

<a href="#">+ Create New</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<input type="text" value="Search"/>	<a href="#">Q</a>
Name	FortiGate	Action	Status	Last Trigger Time
Incoming Webhook				
auto_webhook	All FortiGates	NSX Assign VMware NSX Security Tag	Enabled	2020/04/14 11:28:23

## To configure an automation stitch to assign a security tag to NSX-T VMs in the CLI:

### 1. Configure the NSX SDN connector:

```
config system sdn-connector
  edit "nsx_t25"
    set type nsx
    set server "172.18.64.205"
    set username "admin"
    set password xxxxxx
    set vcenter-server "172.18.64.201"
    set vcenter-username "administrator@vsphere.local"
    set vcenter-password xxxxxx
  next
end
```

### 2. Configure the automation stitch:

```
config system automation-action
  edit "auto_webhook_quarantine-nsx"
    set action-type quarantine-nsx
    set security-tag "automation_tag"
    set sdn-connector "nsx_t25"
  next
end

config system automation-trigger
  edit "auto_webhook"
    set trigger-type event-based
    set event-type incoming-webhook
  next
end

config system automation-stitch
  edit "auto_webhook"
    set status enable
    set trigger "auto_webhook"
```

```

        set action "auto_webhook_quarantine-nsx"
    next
end

```

### 3. In NSX-T, create a cURL request to trigger the automation stitch on the FortiGate:

```

root@pc56:/home# curl -k -X POST -H 'Authorization: Bearer
3fdxNG08mgNg0fh4NQ51g1NQ1QHcxx' --data '{ "srcip": "10.1.30.242"}'
https://172.16.116.230/api/v2/monitor/system/automation-stitch/webhook/auto_webhook
{
  "http_method": "POST",
  "status": "success",
  "http_status": 200,
  "serial": "FGVM08TM20000220",
  "version": "v6.4.0",
  "build": 1608
}

```

### To verify the automation stitch is triggered and the action is executed:

```

# diagnose test application autod 2

csf: enabled root:yes
version:1586883541 sync time:Tue Apr 14 11:04:05 2020

total stitches activated: 1

stitch: auto_webhook
destinations: all
trigger: auto_webhook

(id:15)service=auto_webhook

local hit: 1 relayed to: 0 relayed from: 0
actions:
auto_webhook_quarantine-nsx type:quarantine-nsx interval:0
security tag:automation_tag
sdn connector:
nsx_t25;

```

## FortiNAC quarantine action for automation - 6.4.2

Users can configure an automation stitch with the *Quarantine via FortiNAC* action with a *Compromised Host* or *Incoming Webhook* trigger. When the automation is triggered, the client PC will be quarantined and its MAC address is disabled in the configured FortiNAC.

In this example, the FortiNAC has been configured to join an enabled Security Fabric (see [FortiNAC](#) for more information).

The FortiNAC must also be configured to isolate disabled hosts:

- Endpoints connecting to FortiWiFi or wired ports on FortiGate:
  - See the requisite *Configure FortiNAC* section in the [FortiGate Endpoint Management Integration Guide](#).
- Endpoints connecting to FortiAP:
  - Set the *Dead End VLAN*. See [Model configuration](#).

- Endpoints connecting to FortiSwitch:
  - Set the *Dead End* VLAN. See [Model configuration](#).
  - Add the switch to the physical address filtering group. See [Systems groups](#) and [Modify a group](#).

## To configure a FortiNAC quarantine automation stitch in the GUI:

- Configure the automation stitch:
  - Go to *Security Fabric > Automation* and click *Create New*.
  - In the *Trigger* section, select *Incoming Webhook*.
  - In the *Action* section, select *Quarantine via FortiNAC*.
  - Click *OK*.

Edit Automation Stitch


Name:

Status: Enabled Disabled

FortiGate: All FortiGates +

---

Trigger

 Incoming Webhook

URL:

API admin key:

Sample cURL request: 

```
curl -k -X POST -H 'Authorization: Bearer <API key>' --data '{"srcip": "1.1.1.1", "mac": "11:11:11:11:11:11", "fctuid": "A8BA0B12DA694E47BA4ADF24F8358E2F"}' https://172.17.48.225:4431/api/v2/monitor/system/automation-
```

---

Action

☐ CLI Script
 ☐ Email
 ☐ FortiExplorer Notification
 ☐ Access Layer Quarantine
 ☐ Quarantine FortiClient
 ☒ Quarantine via FortiNAC
 ☐ Assign VMware NSX Security Tag
 ☐ IP Ban
 ☐ AWS Lambda
 ☐ Azure Function
 ☐ Google Cloud Function

☐ AliCloud Function
 ☐ Slack Notification
 ☐ Webhook

Minimum interval (seconds):

OK Cancel

- Create a new API user and generate the API key:
  - Go to *System > Administrators* and click *Create New > REST API Admin*.
  - Configure the settings as needed.

Edit REST API Admin

Username

Comments  0/255

Administrator Profile

API key

PKI Group ☐

CORS Allow Origin ☐

Restrict login to trusted hosts

Trusted Hosts

- c. Click OK. The *New API key* window opens.
- d. Copy the key to the clipboard and click *Close*.
- e. Click OK.

3. Add the API key to the automation stitch:

- a. Go to *Security Fabric > Automation* and edit the automation stitch created in step 1.
- b. Paste the key in the *API admin key* field.
- c. Click OK.


Edit Automation Stitch

Name

Status ☒ Enabled ☐ Disabled

FortiGate

Trigger

 Incoming Webhook


URL


API admin key


Sample cURL request 


```
curl -k -X POST -H
'Authorization: Bearer
ckx7d9xdzx14Nztd1Ncr701dp
wwy9' --data '{"srcip": "1.1.1.1",
"mac": "11:11:11:11:11:11",
"ftcid":
"A8BA0B12DA694E47BA4ADF
24F8358E2F"}'
https://172.17.48.225:4431/api/
v2/monitor/system/automation-
stitch/webhook/auto_webhook
```


Action


 CLI Script


 Email


 FortiExplorer Notification


 Access Layer Quarantine


 Quarantine FortiClient


 Quarantine via FortiNAC


 Assign VMware NSX Security Tag


 IP Ban


 AWS Lambda

 Azure Function

 Google Cloud Function

 AliCloud Function

 Slack Notification

 Webhook

Minimum interval (seconds)

4. On a Linux PC accessible by the FortiGate, create a cURL request to trigger the automation stitch:

```
root@pc56:~# curl -k -X POST -H 'Authorization: Bearer cxx7d9xdzzx14Nztd1Ncr701dpwwy9' --data '{ "srcip": "1.1.1.1", "mac": "00:0C:29:0B:A6:16", "fctuid": "A8BA0B12DA694E47BA4ADF24F8358E2F" }' https://172.17.48.225:4431/api/v2/monitor/system/automation-stitch/webhook/auto_webhook
```

5. In FortiOS, verify the automation stitch is triggered and the action is executed:
  - a. Go to *Log & Report > Events* and select *System Events* to confirm that the stitch was activated.
  - b. Go to *Security Fabric > Automation* to see the last time that the stitch was triggered.

<a href="#">+ Create New</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<input type="text" value="Search"/>	<input type="button" value="Q"/>
Name	FortiGate	Action	Status	Last Trigger Time
Incoming Webhook 1				
auto_webhook	All FortiGates	Quarantine via FortiNAC	Enabled	2020/06/23 15:25:44

In FortiNAC, the *Host View* shows the status of the client PC. It is quarantined and its MAC address is disabled.

FortiNAC-VM-CA * Host View									
<a href="#">Bookmarks</a> <a href="#">Users</a> <a href="#">Hosts</a> <a href="#">Network Devices</a> <a href="#">Logs</a> <a href="#">Policy</a> <a href="#">System</a> <a href="#">Help</a>									
Hosts - Displayed: 1 Total: 7									
Adapter View <b>Host View</b> User View Application View									
Search PC34 << first < prev 1 next > last >> 25									
Status	Host Name	Registered To	Logged On User	Host Role	Operating System	Host Created	Last Modified Date	Last Modified By	
✖	PC34			NAC-Default	Microsoft Windows 7	06/19/20 04:24 AM PDT	06/19/20 09:51 AM PDT	SYSTEM	
Status IP Address Physical Address Media Type Location Connected Container Actions 00:0C:29:0B:A6:16 Wired									
Import Export to Options Add Modify Delete Enable Disable									

## To configure a FortiNAC quarantine automation stitch in the CLI:

1. Configure the automation stitch:

```
config system automation-action
  edit "auto_webhook_quarantine-fortinac"
    set action-type quarantine-fortinac
  next
end

config system automation-trigger
  edit "auto_webhook"
    set event-type incoming-webhook
  next
end

config system automation-stitch
  edit "auto_webhook"
    set trigger "auto_webhook"
    set action "auto_webhook_quarantine-fortinac"
  next
end
```

2. Create a new API user and generate the API key:

```

config system api-user
  edit "g-api-rw-user"
    set api-key ENC SH2SHFEtfJQ9OsfH/keh4kdULAp3V4ps7HkxBuDIzpR4Cmsckaa9wJ6kw28dFQ=
    set accprofile "super_admin"
    set vdom "root"
  config trusthost
    edit 1
      set ipv4-trusthost 10.6.30.0 255.255.255.0
    next
  end
next
end

```

### 3. On a Linux PC accessible by the FortiGate, create a cURL request to trigger the automation stitch:

```

root@pc56:~# curl -k -X POST -H 'Authorization: Bearer cxx7d9xdzzx14Nztd1Ncr701dpwwy9' -
-data '{ "srcip": "1.1.1.1", "mac": "00:0C:29:0B:A6:16", "fctuid":
"A8BA0B12DA694E47BA4ADF24F8358E2F"}'
https://172.17.48.225:4431/api/v2/monitor/system/automation-stitch/webhook/auto_webhook

```

### 4. In FortiOS, verify the automation stitch is triggered and the action is executed:

```

# diagnose test application autod 2
csf: enabled    root:yes
version:1592949233 sync time:Tue Jun 23 15:03:15 2020

total stitches activated: 1

stitch: auto_webhook
  destinations: all
  trigger: auto_webhook

      (id:15)service=auto_webhook

      local hit: 1 relayed to: 0 relayed from: 0
      actions:
        auto_webhook_quarantine-fortinac type:quarantine-fortinac interval:0

date=2020-06-23 time=15:25:44 logdesc="Internal Message" path="system" name="automation-
stitch" action="webhook" mkey="auto_webhook" srcip="1.1.1.1" mac="00:0C:29:0B:A6:16"
fctuid="A8BA0B12DA694E47BA4ADF24F8358E2F" vdom="root" service="auto_webhook"

date=2020-06-23 time=15:25:44 logid="0100046600" type="event" subtype="system"
level="notice" vd="root" eventtime=1592951144401490054 tz="-0700" logdesc="Automation
stitch triggered" stitch="auto_webhook" trigger="auto_webhook" stitchaction="auto_
webhook_quarantine-fortinac" from="log" msg="stitch:auto_webhook is triggered."

```

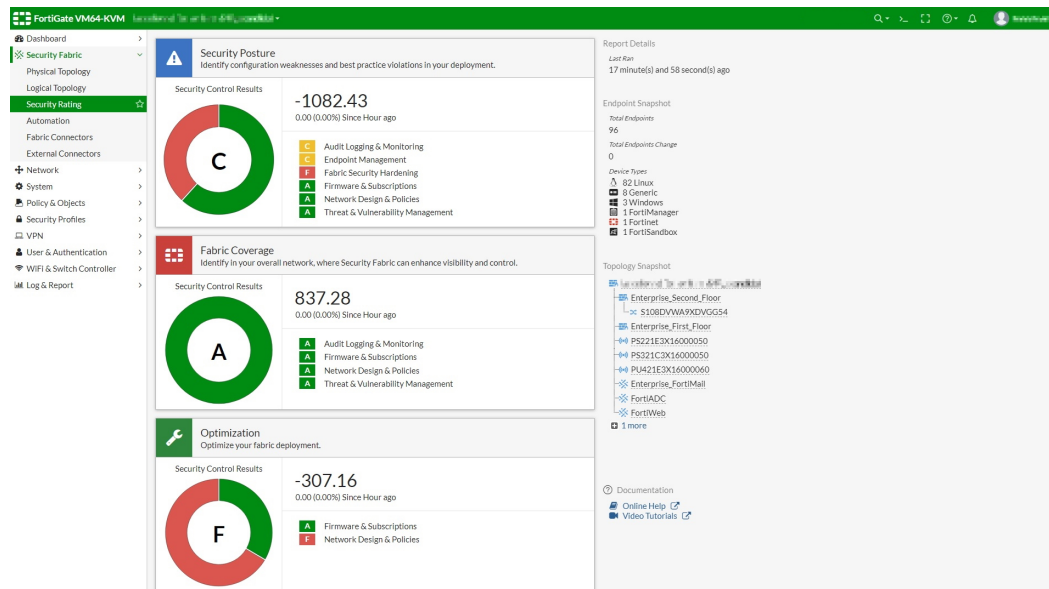
## Security ratings

This section includes information about security rating related new features:

- [Redesign Security Rating scorecards on page 121](#)
- [Tests for FortiSwitch added to Security Rating 6.4.2 on page 122](#)
- [Security rating report in multi VDOM mode 6.4.3 on page 126](#)

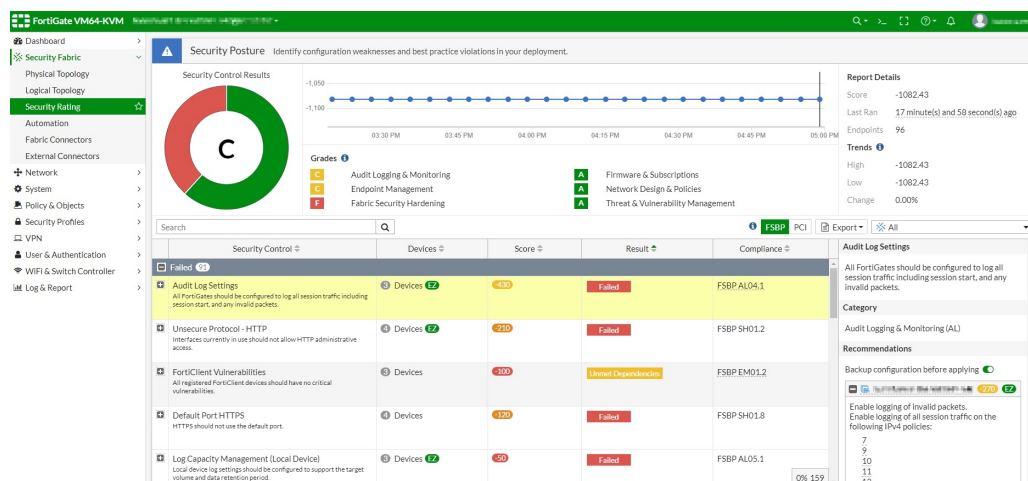
## Redesign Security Rating scorecards

The *Security Rating* page is separated into three major scorecards: *Security Posture*, *Fabric Coverage*, and *Optimization*, which provide an executive summary of the three largest areas of security focus in the Security Fabric.



This page is only visible on the root FortiGate or a standalone FortiGate. It is not visible on downstream FortiGates.

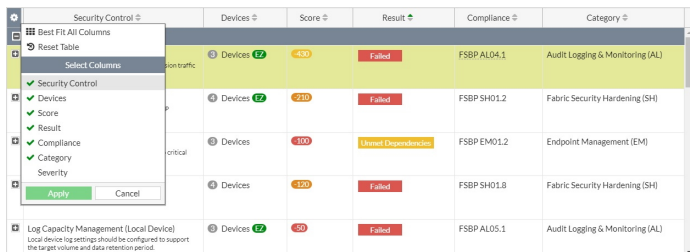
The scorecards show an overall letter grade and breakdown of the performance in sub-categories. Clicking a scorecard drills down to a detailed report of itemized results and compliance recommendations. The point score represents the net score for all passed and failed items in that area. The report includes the security controls that were tested against, linking to specific FSBP or PCI compliance policies. Click the *FSBP* and *PCI* buttons to reference the corresponding standard.



Certain remediations marked with an *EZ* symbol represent configuration recommendations that support *Easy Apply*. In the panel on the right, in the *Recommendations* section, click *Apply* to apply the changes to resolve the failed security control.



The report table can be customized by adding more columns, such as *Category*, to view, filter, or sort the results based on scorecard categories. Click the gear icon to customize the table.



Users can also export the reports as CSV or JSON files by clicking the *Export* dropdown.



To exit the current view, click the icon beside the scorecard title to return to the summary view.

## Security rating check scheduling

Security rating checks by default are scheduled to run automatically every four hours.

### To disable automatic security checks using the CLI:

```
config system global
    security-rating-run-on-schedule disable
end
```

### To manually run a report using the CLI:

```
# diagnose report-runner trigger
```

## Tests for FortiSwitch added to Security Rating - 6.4.2

Six new scenarios have been added in the *Security Rating* to test the FortiSwitch network and make recommendations to optimize the setup.



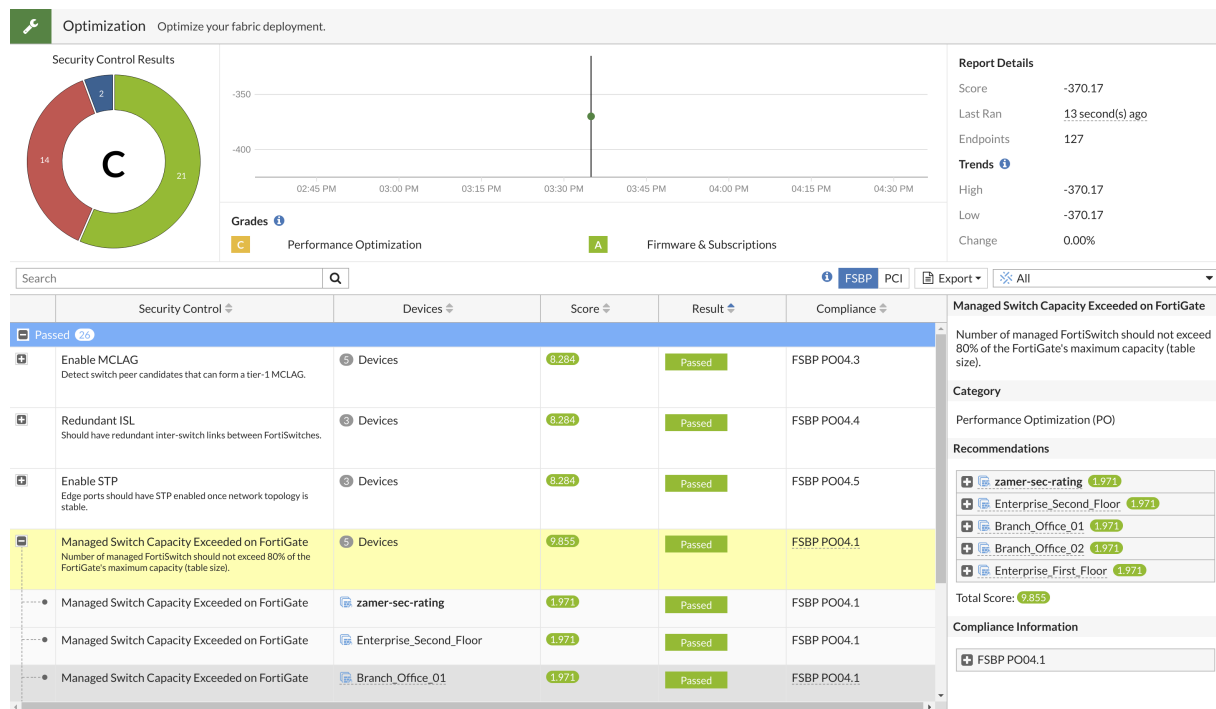
The following tests can be accessed by going to *Security Fabric > Security Rating* and clicking the *Optimization* scorecard.

### Managed Switch Capacity Exceeded on FortiGate:

This test checks for the number of FortiSwitches managed by the downstream FortiGates that have exceeded 80% of the limit. The score is calculated individually and then averaged out. If the number of connected FortiSwitches is equal or greater than the maximum limit, then the result is a fail.

Users can upgrade to higher capacity FortiGates or add more FortiGates to the Security Fabric so the FortiSwitches can be split between multiple FortiGates.

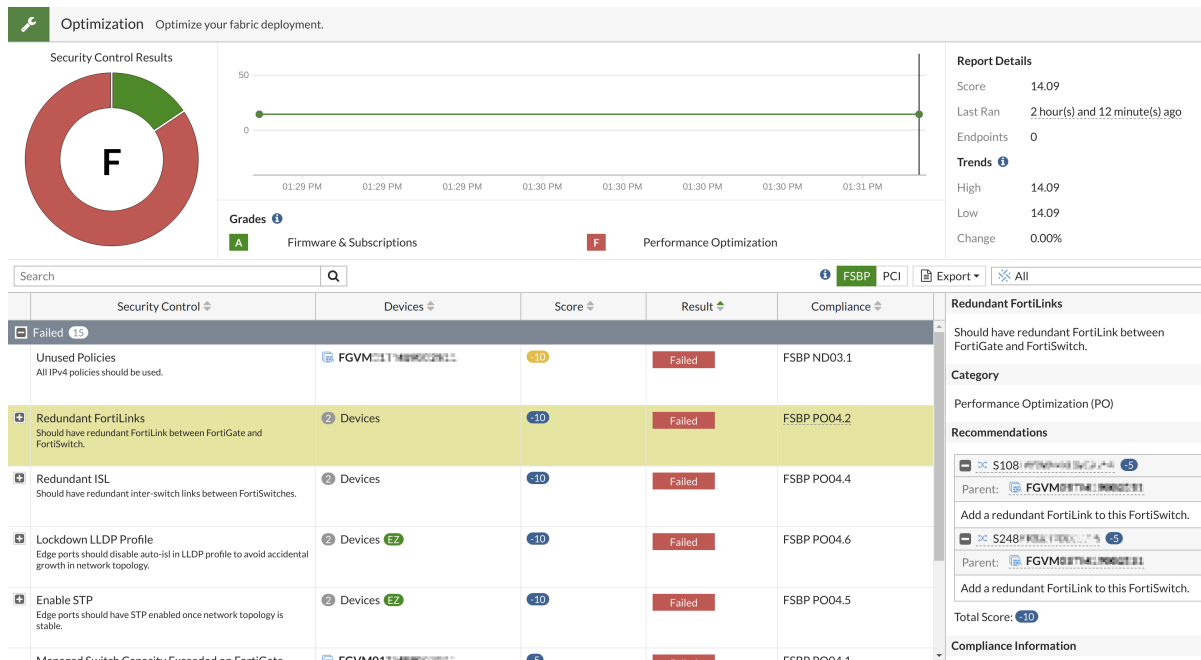
In this example, the downstream FortiGates passed.



### Redundant FortiLinks:

This test checks for redundant FortiLinks between the FortiGate and the FortiSwitch. There are multiple ports dedicated to FortiLink on FortiSwitches directly connected to FortiGates. FortiSwitches that are not directly connected to the FortiGate are exempt from this test. If there are no redundant FortiLinks, then the result is a fail.

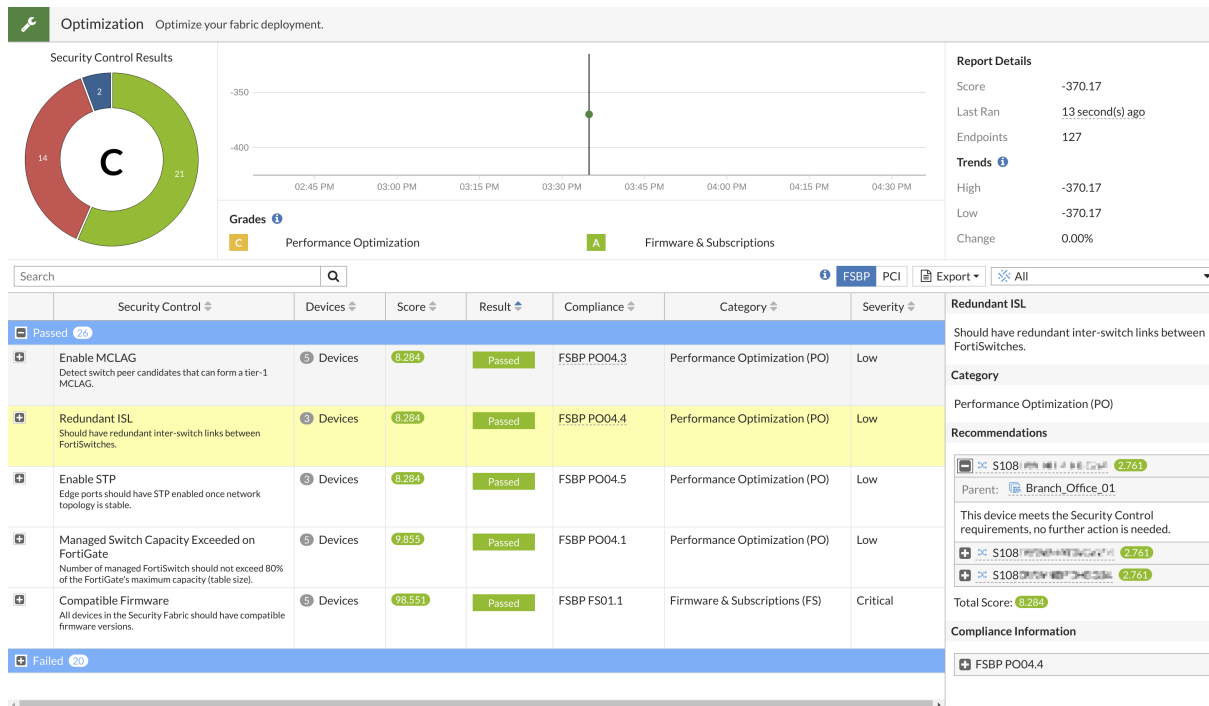
In this example, the FortiGate failed. The *Recommendations* section lists which FortiSwitches require redundant FortiLinks.



## Redundant ISL:

For FortiSwitches with inter-switch links (ISL), this test checks for two redundant links. If there is only one link, then the result is a fail. The *Recommendations* section lists which devices require an additional link. FortiSwitches with inter-chassis links (ICL) are exempt from the test.

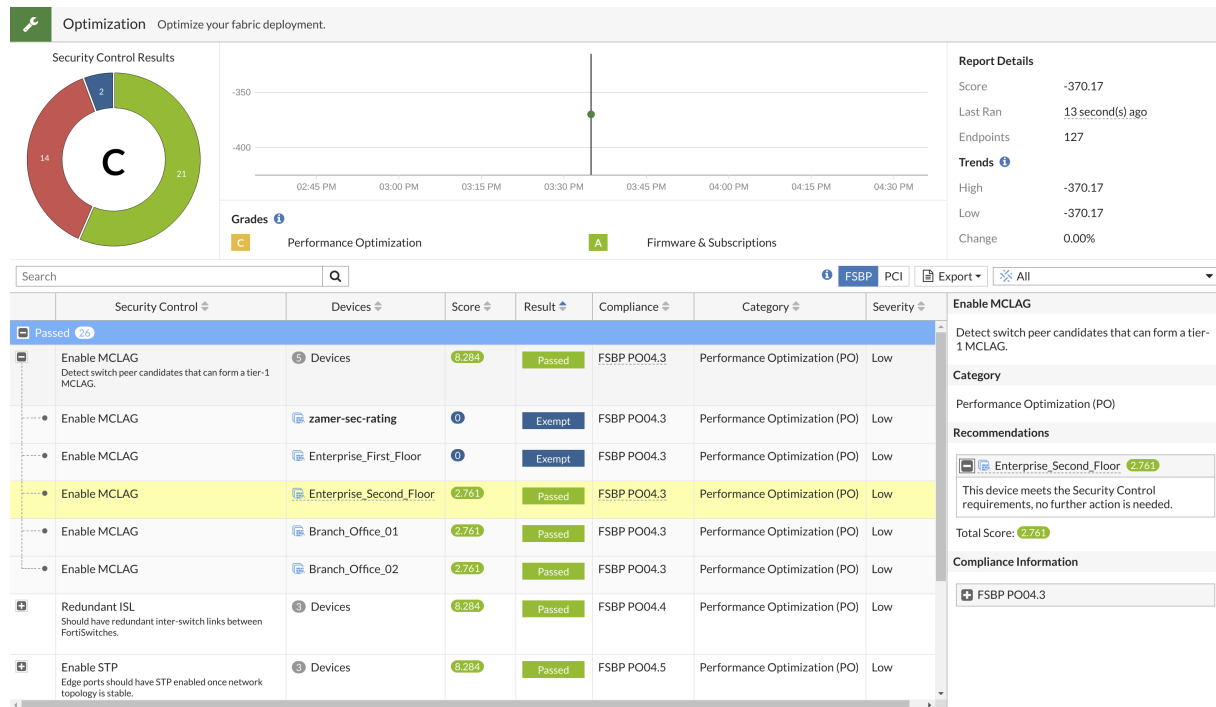
In this example, the devices passed.



## Enable MCLAG:

This test checks for candidate FortiSwitches that can form a tier-1 MCLAG. To do this, the FortiSwitches must be connected to each other and directly connected to the FortiGate. The FortiSwitch must support MCLAG. If an MCLAG already exists, this check is skipped.

In this example, three devices passed the test and two devices were exempt.

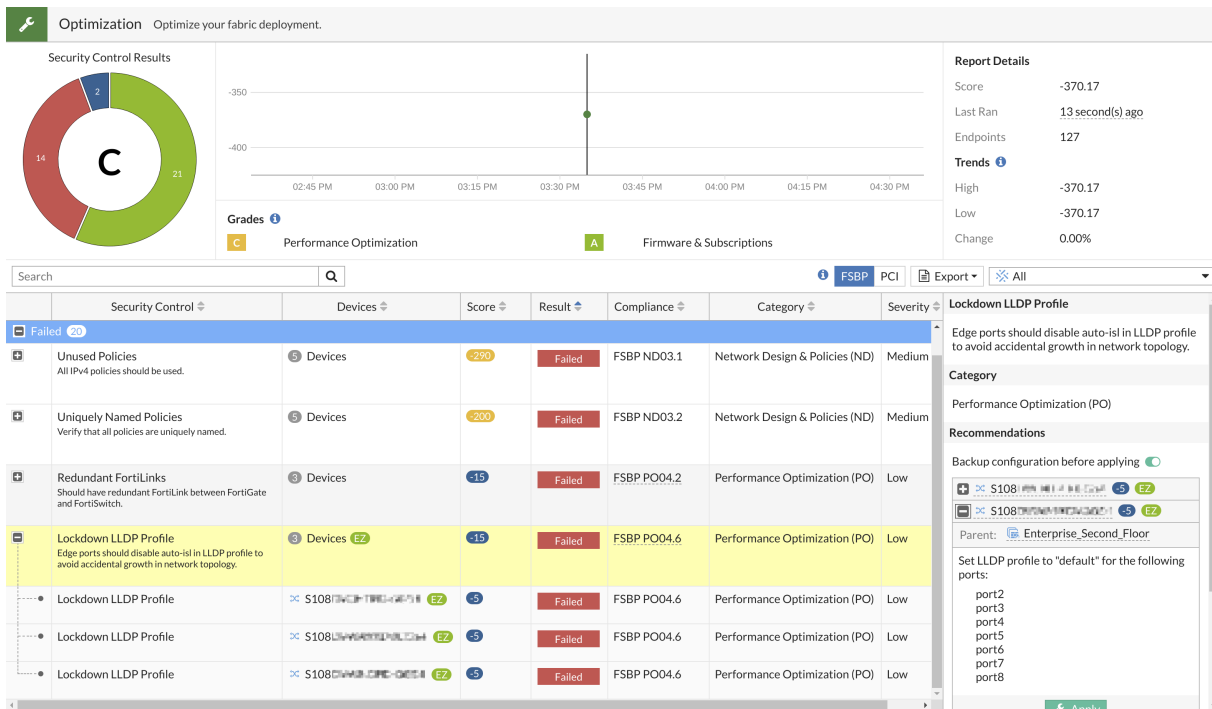


## Lockdown LLDP Profile:

This test ensures that there are no accidental changes to the topology. For edge ports (not FortiLink or ISL), FortiOS suggests using the default LLDP profile. The test verifies the following:

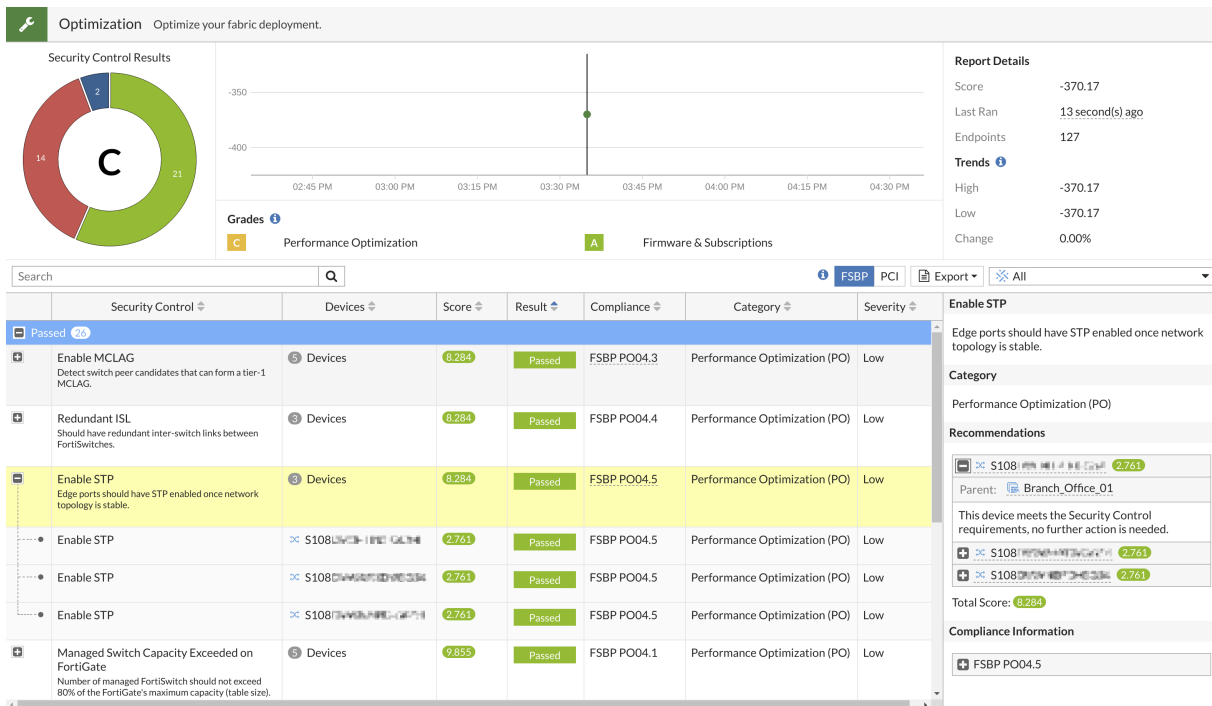
- Looks for an edge port that has an auto-ISL LLDP profile
- Checks if the edge port BPDU guard is disabled
- Check if the FortiGate DHCP server and switches do not have a DHCP key

In this example, the devices failed. The EZ (Easy Apply) symbol appears, and port configurations to optimize the Security Fabric can be applied in the *Recommendations* section.



### Enable STP:

This test checks if STP is enabled on edge ports. Once the network topology is stable, edge ports should have STP enabled to optimize the Security Fabric. In this example, the devices passed.

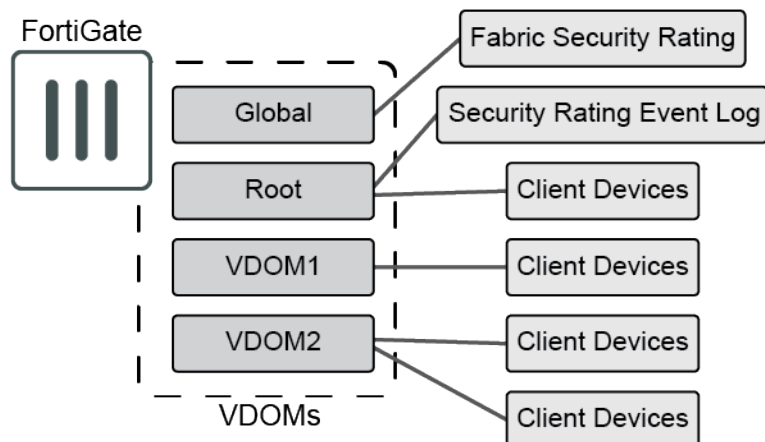


## Security rating report in multi VDOM mode - 6.4.3

In multi VDOM mode, security rating reports can be generated in the Global VDOM for all of the VDOMs on the device. Administrators with read/write access can run the security rating report in the Global VDOM. Administrators with read-only access can only view the report.

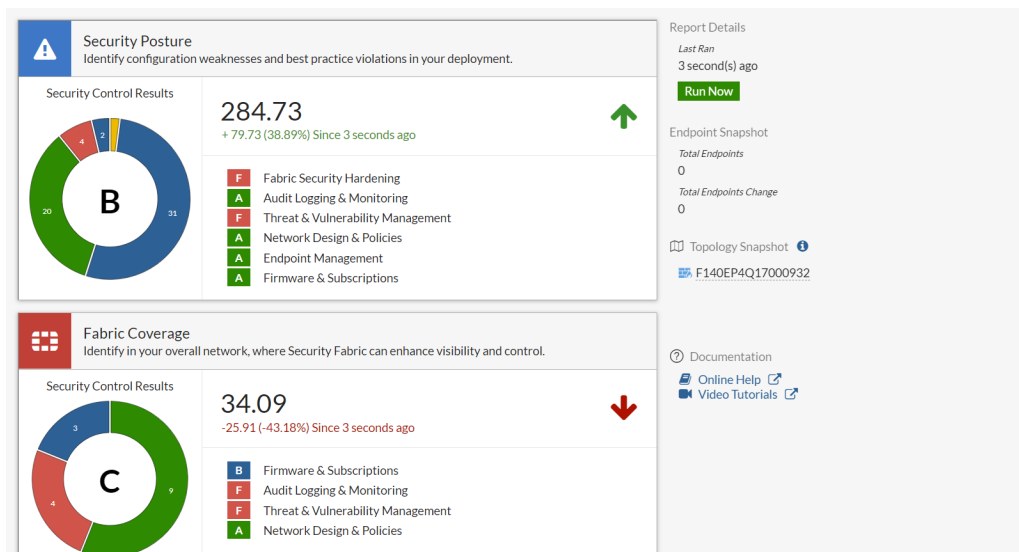
On the report's scorecards, the *Scope* column shows the VDOM or VDOMs that the check was run on. On checks that support *Easy Apply*, the remediation can be run on all of the associated VDOMs.

The security rating event log is available on the root VDOM.



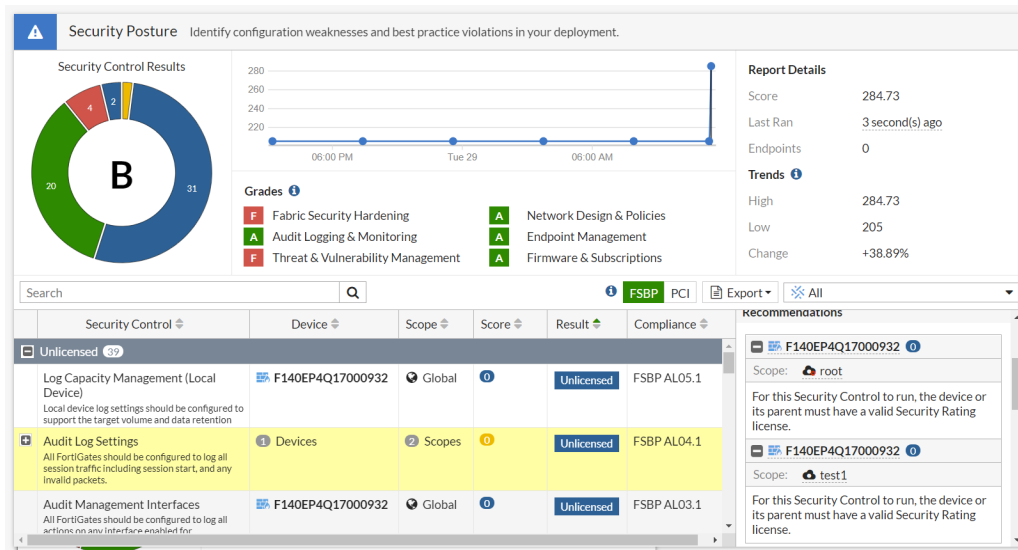
### To run a security rating report for all VDOMs:

1. In the Global VDOM, go to *Security Fabric > Security Rating*.
2. In the right side bar, click *Run Now*. The security report is run for all of the VDOMs.



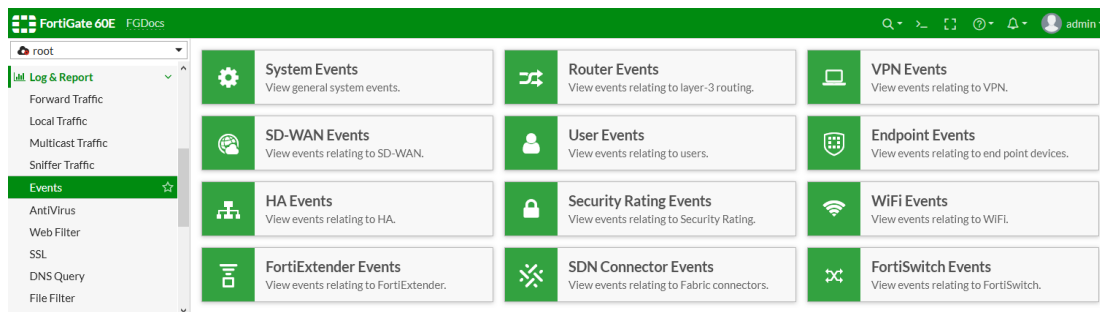
3. Expand a scorecard to view itemized results. The *Scope* column shows the VDOM or VDOMs that the check was

run on.



## To view security rating event logs:

1. In the root VDOM, go to **Log & Report > Events**.



2. Click the **Security Rating Events** subcategory.

Date/Time	Level	Log Description	Result	Security Score	Report
2020/09/29 07:55:39		Security Rating summary	0 0 2 0 11	+205	Security Posture
2020/09/29 07:55:39		Security Rating summary	2 0 1 0 11	+60	Fabric Coverage
2020/09/29 07:55:39		Security Rating summary	0 0 0 0 4	+65	Optimization
2020/09/29 03:45:39		Security Rating summary	0 0 2 0 11	+205	Security Posture
2020/09/29 03:45:39		Security Rating summary	2 0 1 0 11	+60	Fabric Coverage
2020/09/29 03:45:39		Security Rating summary	0 0 0 0 4	+65	Optimization
2020/09/28 23:35:35		Security Rating summary	0 0 2 0 11	+205	Security Posture
2020/09/28 23:35:34		Security Rating summary	2 0 1 0 11	+60	Fabric Coverage
2020/09/28 23:35:34		Security Rating summary	0 0 0 0 4	+65	Optimization
2020/09/28 19:25:35		Security Rating summary	0 0 2 0 11	+205	Security Posture
2020/09/28 19:25:35		Security Rating summary	2 0 1 0 11	+60	Fabric Coverage
2020/09/28 19:25:34		Security Rating summary	0 0 0 0 4	+65	Optimization
2020/09/28 15:15:34		Security Rating summary	0 0 2 0 11	+205	Security Posture
2020/09/28 15:15:34		Security Rating summary	2 0 1 0 11	+60	Fabric Coverage
2020/09/28 15:15:34		Security Rating summary	0 0 0 0 4	+65	Optimization
2020/09/28 14:37:20		Security Rating result change	0 1 1 0 2	+110	Security Posture
2020/09/28 14:37:20		Security Rating summary	0 0 2 0 11	+205	Security Posture
2020/09/28 14:37:20		Security Rating summary	2 0 1 0 11	+60	Fabric Coverage
2020/09/28 14:37:20		Security Rating result change	2 0 1 0 11	+205	Optimization

# Network

This section includes information about network related new features:

- [SD-WAN on page 129](#)
- [General on page 191](#)
- [IPv6 on page 213](#)
- [Web proxy on page 225](#)

## SD-WAN

This section includes information about SD-WAN related new features:

- [SD-WAN event log subtype on page 129](#)
- [SD-WAN logging improvement to identify matched application on page 133](#)
- [SD-WAN configuration portability on page 134](#)
- [SD-WAN log format improvements on page 136](#)
- [SD-WAN monitor on ADVPN shortcuts on page 142](#)
- [SD-WAN GUI and monitoring enhancements on page 143](#)
- [Enhance ADVPN to support UDP hole punching for spokes behind NAT on page 147](#)
- [SD-WAN health check packet enhancement on page 151](#)
- [Weighted round robin for IPsec aggregate tunnels on page 151](#)
- [Default\\_DNS performance SLA profile on page 153](#)
- [Interface speedtest on page 154](#)
- [Support SD-WAN integration with OCVPN on page 156](#)
- [Allow FortiClient to join OCVPN on page 164](#)
- [Support SD-WAN interface as a security zone 6.4.1 on page 168](#)
- [ADVPN hub and spoke VPN Wizard improvements 6.4.2 on page 172](#)
- [Allow MAC addresses to be used in SD-WAN rules and policy routes 6.4.2 on page 176](#)
- [Up to 1024 spokes in OCVPN 6.4.2 on page 177](#)
- [SD-WAN enhancements 6.4.2 on page 178](#)
- [Define SD-WAN duplication rules to duplicate packets on other members of the SD-WAN zone 6.4.2 on page 182](#)
- [Allow packet duplication on SD-WAN based on SD-WAN rules 6.4.3 on page 184](#)
- [BGP additional path limit increased to 255 6.4.3 on page 186](#)
- [SD-WAN IPv6 route tag 6.4.4 on page 186](#)
- [REST API to monitor SD-WAN SLAs for ADVPN shortcuts 6.4.5 on page 188](#)

## SD-WAN event log subtype

A separate log subtype, *SD-WAN*, has been added to *Event* logs. It consists of seven log IDs:

Log ID	Log description
22923	Virtual WAN link status
22924	Virtual WAN link volume status
22925	Virtual WAN link SLA information
22926	Virtual WAN link neighbor status
22927	Virtual WAN link neighbor standalone
22928	Virtual WAN link neighbor primary
22929	Virtual WAN link neighbor secondary

### To filter event logs to show SD-WAN events:

1. Go to **Log & Report > Events**.
2. In the toolbar, click the event dropdown button and select **SD-WAN Events**. The filtered list of SD-WAN event logs appears, including the **Log Description**.
3. Select an entry and click the **Details** button to view more information about the log.

Date/Time	Level	Message	Log Description	Log Details
2019/12/16 16:21:29	Info	SD-WAN Health Check member(s) pass by initialization.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:21:29	Info	Service prioritized by packet-loss will be redirected in seq-num order 1(R150) 2(R160).	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:21:29	Info	Member link is available. Start forwarding traffic.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:21:29	Info	Member link is available. Start forwarding traffic.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:21:29	Info	Member link is available. Start forwarding traffic. Service will be redirected to interface(R160) gateway(2004:10:100:1:5).	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:56	Info	Number of pass members changed. Member 2 out-of-sla.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:36	Info	SD-WAN Health Check member(s) pass by initialization.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:35	Info	Service prioritized by latency will be redirected in seq-num order 2(R160) 1(R150).	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:35	Info	Member link is available. Start forwarding traffic.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:35	Info	Member link is available. Start forwarding traffic.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:35	Info	Member link is available. Start forwarding traffic. Service will be redirected to interface(R160) gateway(2004:10:100:1:5).	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:09	Info	SD-WAN Health Check member(s) pass by initialization.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:08	Info	Service prioritized by latency will be redirected in seq-num order 2(R160) 1(R150).	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:08	Info	Member link is available. Start forwarding traffic.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:08	Info	Member link is available. Start forwarding traffic.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:20:08	Info	Member link is available. Start forwarding traffic. Service will be redirected to interface(R160) gateway(2004:10:100:1:5).	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:19:45	Info	Member link is available. Start forwarding traffic. Service will be redirected to interface(R160) gateway(2004:10:100:1:5).	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:19:45	Info	SD-WAN Health Check member(s) pass by initialization.	Virtual WAN Link status	SD-WAN Events
2019/12/16 16:19:44	Info	SD-WAN health-check member initial state	Virtual WAN Link SLA Information	SD-WAN Events
2019/12/16 16:19:44	Info	SD-WAN health-check member initial state	Virtual WAN Link SLA Information	SD-WAN Events

## Sample SD-WAN event logs

### Virtual WAN Link status

#### Event type = HEALTH CHECK

```
date=2020-03-29 time=16:36:55 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585525015062338339 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Health Check" healthcheck="ping1" slatargetid=1 numpassmember=2 msg="SD-WAN
Health Check member(s) pass."
```

```
date=2020-03-29 time=16:41:30 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585525290513555981 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Health Check" healthcheck="ping1" slatargetid=1 oldvalue="1" newvalue="2"
msg="Number of pass member changed."
```

```
date=2020-03-29 time=16:41:30 logid="0113022923" type="event" subtype="sdwan"
level="information" vd="root" eventtime=1585525290513553153 tz="-0700" logdesc="Virtual WAN
```



```
Link status" eventtype="Health Check" healthcheck="ping1" slatargetid=1 member="2"
msg="Member status changed. Member in sla."
```

```
date=2020-03-29 time=16:40:33 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585525232970358654 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Health Check" healthcheck="ping1" slatargetid=1 member="2" msg="Member status
changed. Member out-of-sla."
```

## Event type = SERVICE

```
date=2020-03-29 time=17:20:13 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585527613995020448 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Service" serviceid=1 service="" metric="latency" seq="1,2" msg="Service
prioritized by performance metric will be redirected in sequence order."
```

```
date=2020-03-29 time=17:20:13 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585527613995017084 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Service" interface="R160" member="2" serviceid=1 service="" gateway="10.100.1.5"
msg="Member link is available. Start forwarding traffic. "
```

```
date=2020-03-29 time=17:33:25 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585528405170900938 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Service" serviceid=1 service="service1" msg="Service disabled caused by no
outgoing path."
```

```
date=2020-03-29 time=17:33:25 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585528405170876948 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Service" serviceid=1 service="service1" msg="Service failover to other available
interface(s)."
```

```
date=2020-03-29 time=17:33:25 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585528405170874263 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Service" interface="R150" member="1" serviceid=1 service="service1"
gateway="10.100.1.1" msg="Member link is unreachable or miss threshold. Stop forwarding
traffic. "
```

```
date=2020-03-29 time=18:05:14 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585530314708843222 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Service" interface="R150" member="1" serviceid=1 service="service1"
gateway="10.100.1.1" metric="packet-loss" oldvalue="1" newvalue="2" msg="The member order
changed by performance metric."
```

```
date=2020-03-29 time=19:25:40 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585535140122779004 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Service" serviceid=1 service="service1" seq="1,2" msg="Service prioritized by SLA
will be redirected in sequence order."
```

```
date=2020-03-29 time=19:27:02 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585535222140485480 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Service" interface="R150" member="1" serviceid=1 service="service1"
gateway="10.100.1.1" oldvalue="1" newvalue="2" msg="The member SLA order changed."
```

```
date=2020-03-29 time=19:38:33 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585535913042763548 tz="-0700" logdesc="Virtual WAN Link status"
eventtype="Service" serviceid=1 service="service1" member="1(R150),2(R160)" msg="Service
will be load balanced among members with available routing."
```

```
date=2020-03-29 time=20:58:50 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585540730662430230 tz="-0700" logdesc="Virtual WAN Link status"
```

```
eventtype="Service" serviceid=1 service="service1" msg="Service disabled caused by role mismatch."
```

## Virtual WAN Link volume status

### Event type = VOLUME

```
date=2020-03-29 time=20:46:19 logid="0113022924" type="event" subtype="sdwan" level="notice" vd="root" eventtime=1585539979756723714 tz="-0700" logdesc="Virtual WAN Link volume status" eventtype="Volume" interface="port12" member="2" msg="Member enters into conservative status with limited ability to receive new sessions for too much traffic."
```

```
date=2020-03-29 time=20:46:19 logid="0113022924" type="event" subtype="sdwan" level="notice" vd="root" eventtime=1585539979756723714 tz="-0700" logdesc="Virtual WAN Link volume status" eventtype="Volume" interface="wan1" member="2" msg="Member resumes normal status to receive new sessions for internal adjustment."
```

## Virtual WAN Link SLA information

### Event type = SLA

```
date=2020-03-29 time=16:51:27 logid="0113022925" type="event" subtype="sdwan" level="notice" vd="root" eventtime=1585525888177637570 tz="-0700" logdesc="Virtual WAN Link SLA information" eventtype="SLA" healthcheck="ping1" slatargetid=1 interface="R150" status="up" latency="0.013" jitter="0.001" packetloss="100.000%" inbandwidth="0kbps" outbandwidth="0kbps" bibandwidth="0kbps" slamap="0x0" metric="packetloss" msg="Health Check SLA status. SLA failed due to being over the performance metric threshold."
```

```
date=2020-03-29 time=16:51:21 logid="0113022925" type="event" subtype="sdwan" level="information" vd="root" eventtime=1585525881177944788 tz="-0700" logdesc="Virtual WAN Link SLA information" eventtype="SLA" healthcheck="ping1" slatargetid=1 interface="R160" status="up" latency="0.010" jitter="0.001" packetloss="0.000%" inbandwidth="0kbps" outbandwidth="0kbps" bibandwidth="0kbps" slamap="0x1" msg="Health Check SLA status."
```

### Event type = HEALTH CHECK

```
date=2020-03-29 time=16:36:54 logid="0113022925" type="event" subtype="sdwan" level="notice" vd="root" eventtime=1585525014564428201 tz="-0700" logdesc="Virtual WAN Link SLA information" eventtype="Health Check" healthcheck="ping1" interface="R160" probepproto="ping" oldvalue="" newvalue="alive" msg="SD-WAN health-check member initial state."
```

```
date=2020-03-29 time=16:55:18 logid="0113022925" type="event" subtype="sdwan" level="warning" vd="root" eventtime=1585526118334582737 tz="-0700" logdesc="Virtual WAN Link SLA information" eventtype="Health Check" healthcheck="ping1" interface="R150" probepproto="ping" oldvalue="alive" newvalue="die" msg="SD-WAN health-check member changed state."
```

```
date=2020-03-29 time=16:54:35 logid="0113022925" type="event" subtype="sdwan" level="notice" vd="root" eventtime=1585526075811696627 tz="-0700" logdesc="Virtual WAN Link SLA information" eventtype="Health Check" healthcheck="ping1" interface="R150" probepproto="ping" oldvalue="die" newvalue="alive" msg="SD-WAN health-check member changed state."
```

## Virtual WAN Link Neighbor

### Event type = NEIGHBOR

```
date=2020-03-29 time=20:57:36 logid="0113022926" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585540656722222479 tz="-0700" logdesc="Virtual WAN Link Neighbor
status" eventtype="Neighbor" neighbor="10.100.1.1" member="1" msg="Neighbor(10.100.1.1) for
member(1) is unselected forcefully due to configuration change."
```

```
date=2020-03-29 time=20:58:51 logid="0113022928" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585540731163096946 tz="-0700" logdesc="Virtual WAN Link Neighbor
primary" eventtype="Neighbor" oldvalue="standalone" newvalue="primary" msg="Selected role is
changed."
```

```
date=2020-03-29 time=20:58:51 logid="0113022926" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585540731163094572 tz="-0700" logdesc="Virtual WAN Link Neighbor
status" eventtype="Neighbor" neighbor="10.100.1.1" member="1" msg="Neighbor(10.100.1.1) for
member(1) is selected."
```

```
date=2020-03-29 time=21:01:01 logid="0113022929" type="event" subtype="sdwan"
level="warning" vd="root" eventtime=1585540861280903746 tz="-0700" logdesc="Virtual WAN Link
Neighbor secondary" eventtype="Neighbor" oldvalue="primary" newvalue="secondary"
msg="Selected role is changed."
```

```
date=2020-03-29 time=21:01:01 logid="0113022926" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1585540861280842811 tz="-0700" logdesc="Virtual WAN Link Neighbor
status" eventtype="Neighbor" neighbor="10.100.1.1" member="1" msg="Neighbor(10.100.1.1) for
member(1) is unselected."
```

## SD-WAN logging improvement to identify matched application

In SD-WAN rules, users can define destinations based on applications. With this enhancement, the `vwlservice` field in the forward traffic log has been updated to include the matched application.

### Sample log

```
183: date=2020-01-17 time=16:48:40 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="root" eventtime=1579308520544853557 tz="-0800" srcip=192.168.1.222
srcport=51530 srcintf="port10" srcintfrole="undefined" dstip=172.217.3.193 dstport=443
dstintf="port9" dstintfrole="undefined" sessionid=12654 proto=6 action="close" policyid=1
policytype="policy" poluuid="7d67e686-3924-51ea-c519-50884240bb75" policyname="1"
service="HTTPS" dstcountry="United States" srccountry="Reserved" trandisp="snat"
transip=172.16.200.1 transport=51530 appid=31077 app="YouTube" appcat="Video/Audio"
apprisk="elevated" applist="g-wifi-default" duration=1 sentbyte=597 rcvdbyte=319 sentpkt=8
rcvdpkt=4 vwlid=2 vwlservice="YouTube" vwlquality="Seq_num(2), alive, selected"
utmaction="allow" countapp=1 utmref=65422-94
```

### To view SD-WAN logs in the GUI:

1. Go to **Log & Report > Forward Traffic**. The **SD-WAN Internet Service** column displays the application.
2. Select a log entry to view the details.

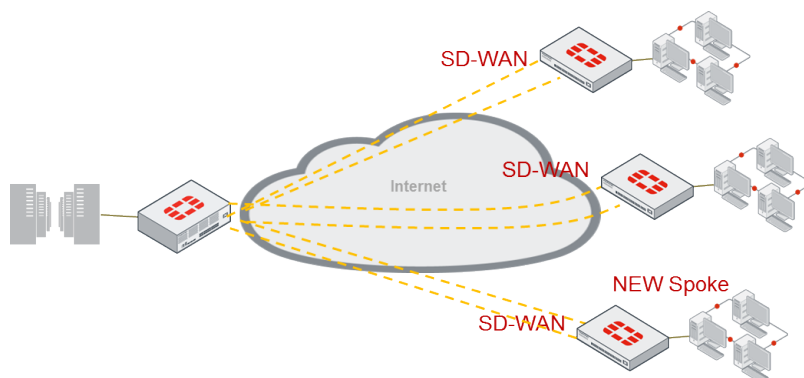
Date/Time	%	Source	Device	Destination	Application Name	Result	Policy	SD-WAN Internet Service	Log Details
2020/01/17 16:48:43		192.168.1.222		172.217.14.206 (www.youtube.com)	YouTube	✓ 27.03 KB / 3.35 KB	1 (1)		Details
2020/01/17 16:48:43		192.168.1.222		104.36.113.23 (image6.pubmatic.com)	HTTPS.BROWSER	✓ 710 B / 4.34 KB	1 (1)		Security
2020/01/17 16:48:41		192.168.1.222		104.36.113.23 (image6.pubmatic.com)	HTTPS.BROWSER	✓ 750 B / 4.34 KB	1 (1)		
2020/01/17 16:48:40		192.168.1.222		172.217.3.193 (yt3.ggpht.com)	YouTube	✓ 597 B / 319 B	1 (1)	YouTube	
2020/01/17 16:48:40		192.168.1.222		172.217.3.193 (yt3.ggpht.com)	YouTube	✓ 597 B / 319 B	1 (1)	YouTube	
2020/01/17 16:48:40		192.168.1.222		172.217.3.193 (yt3.ggpht.com)	YouTube	✓ 597 B / 319 B	1 (1)	YouTube	
2020/01/17 16:48:40		192.168.1.222		172.217.3.193 (yt3.ggpht.com)	YouTube	✓ 597 B / 319 B	1 (1)	YouTube	
2020/01/17 16:48:40		192.168.1.222		172.217.3.193 (yt3.ggpht.com)	YouTube	✓ 597 B / 319 B	1 (1)	YouTube	
2020/01/17 16:48:40		192.168.1.222		172.16.100.100	DNS	✓ 58 B / 247 B	1 (1)		
2020/01/17 16:48:40		192.168.1.222		172.16.100.100	DNS	✓ 58 B / 243 B	1 (1)		
2020/01/17 16:48:39		192.168.1.222		172.217.3.193 (yt3.ggpht.com)	YouTube	✓ 4.28 KB / 27.07 KB	1 (1)		
2020/01/17 16:48:39		192.168.1.222		172.217.3.193 (yt3.ggpht.com)	YouTube	✓ 4.84 KB / 20.07 KB	1 (1)		
2020/01/17 16:48:33		192.168.1.222		172.16.100.100	DNS	✓ 58 B / 202 B	1 (1)		
2020/01/17 16:48:33		192.168.1.222		172.16.100.100	DNS	✓ 58 B / 175 B	1 (1)		

## SD-WAN configuration portability

When configuring SD-WAN, adding interfaces to members is optional. This allows a configuration to be copied directly from one device to another, without requiring the devices to have interfaces with the same names.

After the configuration is pasted to the new device, add the interfaces to the new device to make it fully functional.

### Example



### To copy the SD-WAN configuration from an existing spoke to a new spoke:

1. Copy the configuration from the configured spoke:

```
config system virtual-wan-link
set status enable
```

```
config members
    edit 1
        set interface "_OCVPN3-0.0"
    next
    edit 2
        set interface "_OCVPN3-0.1"
    next
end
config health-check
    edit "office"
        set server "office365.com"
        set protocol http
        set sla-fail-log-period 300
        set sla-pass-log-period 300
        set members 2 1
        config sla
            edit 1
                set latency-threshold 300
                set jitter-threshold 200
            next
            edit 2
                set link-cost-factor latency
                set latency-threshold 20
            next
        end
    next
    ...
end
config service
    edit 2
        set name "Office365"
        set mode sla
        set internet-service enable
        set internet-service-app-ctrl 327782
        config sla
            edit "office"
                set id 1
            next
        end
        set priority-members 2 1
    next
    ...
end
end
```

## 2. Paste the configuration onto the new spoke:

```
config system virtual-wan-link
    set status enable
    config members
        edit 1
        next
        edit 2
        next
    end
    config health-check
```

```

edit "office"
    set server "office365.com"
    set protocol http
    set sla-fail-log-period 300
    set sla-pass-log-period 300
    set members 2 1
    config sla
        edit 1
            set latency-threshold 300
            set jitter-threshold 200
        next
        edit 2
            set link-cost-factor latency
            set latency-threshold 20
        next
    end
next
...
end
config service
    edit 2
        set name "Office365"
        set mode sla
        set internet-service enable
        set internet-service-app-ctrl 327782
        config sla
            edit "office"
                set id 1
            next
        end
        set priority-members 2 1
    next
    ...
end
end

```

The member interfaces are not copied over. Already configured interfaces are not unset. The member is disabled until an interface is configured.

### 3. Configure the member interfaces on the new spoke:

```

config system virtual-wan-link
    config members
        edit 1
            set interface "_OCVPN4-0.0"
        next
        edit 2
            set interface "_OCVPN4-0.1"
        next
    end
end

```

After the interfaces are configured, the new spoke will function like the other spokes.

## SD-WAN log format improvements

The SD-WAN log format has been improved for better reporting and event handler creation on FortiAnalyzer.

## Sample logs

The following sample logs identify where the improvements were made to the log format.

### Service field

The `service` field only includes the service name. The service ID was removed from the `service` field and added to a new field named `serviceid`.

#### Old Format

```
date=2019-11-05 time=12:11:16 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1569438676644424772 tz="-0700" logdesc="Virtual
WAN Link status" eventtype="Service" service="1(gmail)" msg="Service prioritized by
latency will be redirected in seq-num order 1(lan2) 2(wan1)"
```

#### New format

```
date=2020-02-04 time=15:24:23 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580858663336645512 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Service" serviceid=1 service="gmail" metric="latency"
seq="2,1" msg="Service prioritized by performance metric will be redirected in
sequence order."
```

### Name field

The `name` field has been replaced with the more specific `healthcheck` field to be consistent with other logs and to reduce confusion.

#### Old format

```
date=2019-11-03 time=17:13:28 logid="0113022925" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1569284008246643001 tz="-0700" logdesc="Virtual
WAN Link SLA information" eventtype="SLA" name="test" interface="lan2" status="down"
latency="0.000" jitter="0.000" packetloss="85.000%" inbandwidth="0kbps"
outbandwidth="0kbps" bibandwidth="0kbps" slamap="0x0" msg="Health Check SLA status.
SLA 1 failed due to being over the packetloss threshold "
```

#### New format

```
date=2020-02-04 time=14:39:08 logid="0113022925" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580855948407682526 tz="-0800" logdesc="Virtual
WAN Link SLA information" eventtype="SLA" healthcheck="ping1" slatargetid=1
interface="R160" status="up" latency="0.010" jitter="0.000" packetloss="21.000%"
inbandwidth="0kbps" outbandwidth="0kbps" bibandwidth="0kbps" slamap="0x0"
metric="packetloss" msg="Health Check SLA status. SLA failed due to being over the
performance metric threshold."
```

#### Old format

```
date=2019-11-06 time=17:26:12 logid="0113022925" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1569543972762277480 tz="-0700" logdesc="Virtual
WAN Link SLA information" eventtype="Health Check" name="test-1-VIRTUAL_WAN_LINK-1"
interface="lan2" probepproto="ping" oldstate="die" newstate="alive" msg="SD-WAN
health-check member changed state"
```

#### New format

```
date=2020-02-04 time=14:14:42 logid="0113022925" type="event" subtype="sdwan"
level="warning" vd="root" eventtime=1580854483005525076 tz="-0800" logdesc="Virtual
WAN Link SLA information" eventtype="Health Check" healthcheck="ping1-2-VIRTUAL_WAN_
LINK-2" interface="R160" probepproto="ping" oldvalue="alive" newvalue="die" msg="SD-
WAN health-check member changed state."
```

### SLA field

The `sla` field has been replaced with the more specific `slatargetid` field.

#### Old format

```
date=2019-11-06 time=16:51:05 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1573087865540014616 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Health Check" healthcheck="ping2" sla="22"
oldpassmember="2" newpassmember="1" msg="Number of pass members changed. Member 2
out-of-sla"
```

#### New format

```
date=2020-02-04 time=14:38:16 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580855896895319923 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Health Check" healthcheck="ping1" slatargetid=1
oldvalue="2" newvalue="1" msg="Number of pass member changed." date=2020-02-04
time=14:38:16 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1580855896895316020 tz="-0800" logdesc="Virtual WAN Link status"
eventtype="Health Check" healthcheck="ping1" slatargetid=1 member="2" msg="Member
status changed. Member out-of-sla."
```

### SLA ID

The SLA ID was moved from the `msg` field and added to the new `slatargetid` field. The SLA values were also removed from the `msg` field. There is now one log for each SLA failure.

#### Old format

```
date=2019-12-06 time=10:19:53 logid="0113022925" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1575656393121996604 tz="-0800" logdesc="Virtual
WAN Link SLA information" eventtype="SLA" name="1" interface="port1" status="up"
latency="0.092" jitter="0.006" packetloss="0.000%" inbandwidth="99.98Mbps"
outbandwidth="99.99Mbps" bibandwidth="199.97Mbps" slamap="0x0" msg="Health Check SLA
status. SLA 1 failed due to being over the latency threshold SLA 2 failed due to
being over the jitter threshold"
```



**New format**

```
date=2020-02-05 time=15:56:27 logid="0113022925" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580946987433804652 tz="-0800" logdesc="Virtual
WAN Link SLA information" eventtype="SLA" healthcheck="ping1" slatargetid=2
interface="R160" status="up" latency="3.012" jitter="1.002" packetloss="43.000%"
inbandwidth="0kbps" outbandwidth="0kbps" bibandwidth="0kbps" slamap="0x0"
metric="latency" msg="Health Check SLA status. SLA failed due to being over the
performance metric threshold." date=2020-02-05 time=15:56:27 logid="0113022925"
type="event" subtype="sdwan" level="notice" vd="root" eventtime=1580946987433799366
tz="-0800" logdesc="Virtual WAN Link SLA information" eventtype="SLA"
healthcheck="ping1" slatargetid=1 interface="R160" status="up" latency="3.012"
jitter="1.002" packetloss="43.000%" inbandwidth="0kbps" outbandwidth="0kbps"
bibandwidth="0kbps" slamap="0x0" metric="jitter" msg="Health Check SLA status. SLA
failed due to being over the performance metric threshold."
```

**Old and new value fields**

The *old* and *new* value field types have been replaced with the `oldvalue` and `newvalue` fields since the field values are meaningful enough to cover different log types.

**Old format**

```
date=2019-11-05 time=15:08:07 logid="0113022927" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1569449287861854771 tz="-0700" logdesc="Virtual
WAN Link Neighbor standalone" eventtype="Neighbor" oldselectedrole="primary"
newselectedrole="standalone" msg="Selected role is changed."
```

**New format**

```
date=2020-02-04 time=17:09:57 logid="0113022927" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580864997042080958 tz="-0800" logdesc="Virtual
WAN Link Neighbor standalone" eventtype="Neighbor" oldvalue="primary"
newvalue="standalone" msg="Selected role is changed."
```

**Old format**

```
date=2019-11-06 time=16:51:05 logid="0113022925" type="event" subtype="sdwan"
level="warning" vd="root" eventtime=1573087865315149386 tz="-0800" logdesc="Virtual
WAN Link SLA information" eventtype="Health Check" name="test2-2-VIRTUAL_WAN_LINK-2"
interface="port15" probepROTO="ping" oldstate="alive" newstate="die" msg="SD-WAN
health-check member changed state"
```

**New format**

```
date=2020-02-04 time=14:14:42 logid="0113022925" type="event" subtype="sdwan"
level="warning" vd="root" eventtime=1580854483005525076 tz="-0800" logdesc="Virtual
WAN Link SLA information" eventtype="Health Check" healthcheck="ping1-2-VIRTUAL_WAN_
LINK-2" interface="R160" probepROTO="ping" oldvalue="alive" newvalue="die" msg="SD-
WAN health-check member changed state."
```

**Old format**

```
date=2019-11-04 time=17:28:11 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1569371291676959641 tz="-0700" logdesc="Virtual
WAN Link status" eventtype="Health Check" healthcheck="test" sla="1"
oldpassmember="1" newpassmember="0" msg="Number of pass members changed. Member 2
out-of-sla"
```

**New format**

```
date=2020-02-04 time=17:17:34 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580865454841077461 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Health Check" healthcheck="ping1" slatargetid=1
oldvalue="2" newvalue="1" msg="Number of pass member changed." date=2020-02-04
time=17:17:34 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1580865454841074245 tz="-0800" logdesc="Virtual WAN Link status"
eventtype="Health Check" healthcheck="ping1" slatargetid=1 member="1" msg="Member
status changed. Member out-of-sla."
```

**Network performance metrics**

The latency, jitter, and packet loss network performance metrics were removed from the `msg` field and moved to a new field named `metric`. The cause factor has also been removed from the `msg` field.

**Old format**

```
date=2019-11-05 time=16:22:00 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1572999721054428968 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Service" service="2(rule12)" msg="Service prioritized by
latency will be redirected in seq-num order 2(port15) 1(port13)."
```

**New format**

```
date=2020-02-04 time=15:24:23 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580858663336645512 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Service" serviceid=1 service="gmail" metric="latency"
seq="2,1" msg="Service prioritized by performance metric will be redirected in
sequence order."
```

**Old format**

```
date=2019-11-05 time=12:11:16 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1569438676644407292 tz="-0700" logdesc="Virtual
WAN Link status" eventtype="Service" interface="wan1" member="2" service="1(gmail)"
msg="The member link quality latency order changed from 1 to 2."
```

**New format**

```
date=2020-02-04 time=15:40:48 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580859648553624138 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Service" interface="R160" member="2" serviceid=1
service="gmail" gateway="10.100.1.5" metric="packet-loss" oldvalue="1" newvalue="2"
msg="The member order changed by performance metric."
```

## Gateway address

The `gateway` address has been removed from the `msg` field and added to a new field named `gateway`.

### Old format

```
date=2019-11-07 time=07:49:58 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1569595798367258194 tz="-0700" logdesc="Virtual
WAN Link status" eventtype="Service" interface="wan1" member="2" service="2(is)"
msg="Member link is available. Start forwarding traffic. Service will be redirected
to interface(wan1) gateway(172.18.45.1)"
```

### New format

```
date=2020-02-04 time=15:39:04 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580859544464985538 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Service" interface="R160" member="2" serviceid=2
service="google-isdb" gateway="10.100.1.5" msg="Member link is available. Start
forwarding traffic. "
```

## Seq-num order

The `seq-num` order was removed from the `msg` field and added to the new field named `seq`. The order values were also removed from the `msg` field.

### Old format

```
date=2019-11-05 time=16:22:00 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1572999721054428968 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Service" service="2(rule12)" msg="Service prioritized by
latency will be redirected in seq-num order 2(port15) 1(port13)"
```

### New format

```
date=2020-02-04 time=15:39:04 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580859544464944421 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Service" serviceid=1 service="gmail" metric="latency"
seq="2,1" msg="Service prioritized by performance metric will be redirected in
sequence order."
```

## Member value

The member value was removed from the `msg` field and added to the `member` field. There is now one log for each changed member and another log for how the pass member changed.

### Old format

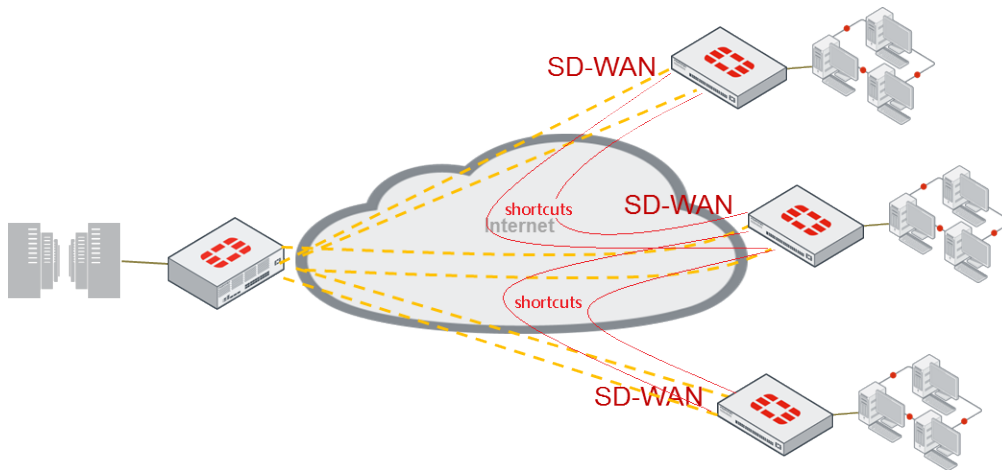
```
date=2019-12-11 time=14:47:40 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1576104460831070527 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Health Check" healthcheck="test" sla="22"
oldpassmember="2" newpassmember="1" msg="Number of pass members changed. Member 2
out-of-sla"
```

**New format**

```
date=2020-02-04 time=17:17:34 logid="0113022923" type="event" subtype="sdwan"
level="notice" vd="root" eventtime=1580865454841077461 tz="-0800" logdesc="Virtual
WAN Link status" eventtype="Health Check" healthcheck="ping1" slatargetid=1
oldvalue="2" newvalue="1" msg="Number of pass member changed." date=2020-02-04
time=17:17:34 logid="0113022923" type="event" subtype="sdwan" level="notice"
vd="root" eventtime=1580865454841074245 tz="-0800" logdesc="Virtual WAN Link status"
eventtype="Health Check" healthcheck="ping1" slatargetid=1 member="1" msg="Member
status changed. Member out-of-sla."
```

**SD-WAN monitor on ADVPN shortcuts**

SD-WAN monitors ADVPN shortcut link quality by dynamically creating link monitors for each ADVPN link. The dynamic link monitor on the spoke will use ICMP probes and the IP address of the gateway as the monitored server. These ICMP probes will not be counted as actual user traffic that keeps the spoke-to-spoke tunnel alive.



- When no shortcut is established:

```
# diagnose sys virtual-wan-link health-check
Health Check(ping):
Seq(1 tunnel-1): state(alive), packet-loss(0.000%) latency(0.038), jitter(0.006) sla_
map=0x3
Seq(2 tunnel-2): state(alive), packet-loss(0.000%) latency(0.035), jitter(0.004) sla_
map=0x3
```

- When one shortcut is established:

```
# diagnose sys virtual-wan-link health-check
Health Check(ping):
Seq(1 tunnel-1): state(alive), packet-loss(0.000%) latency(0.039), jitter(0.003) sla_
map=0x3
Seq(1 tunnel-1_0): state(alive), packet-loss(0.000%) latency(0.060), jitter(0.023) sla_
map=0x3
Seq(2 tunnel-2): state(alive), packet-loss(0.000%) latency(0.035), jitter(0.002) sla_
map=0x3
```

- When more than one shortcut is established:

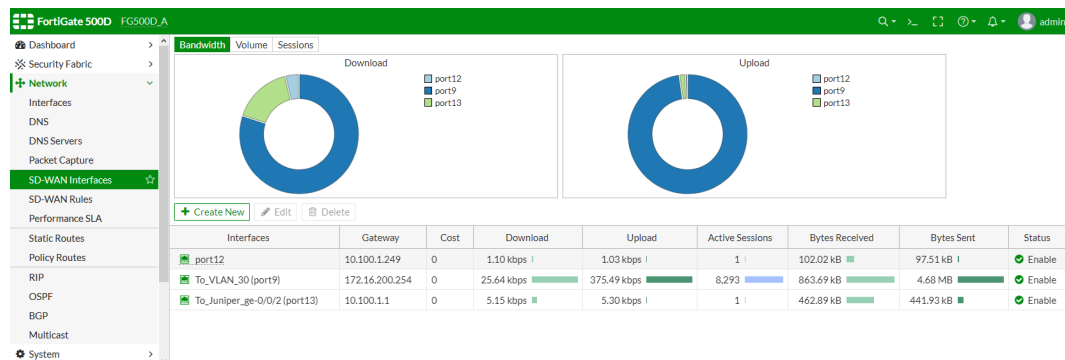
```
# diagnose sys virtual-wan-link health-check
Health Check(ping):
Seq(1 tunnel-1): state(alive), packet-loss(0.000%) latency(0.036), jitter(0.004) sla_
map=0x3
Seq(1 tunnel-1_0): state(alive), packet-loss(0.000%) latency(0.041), jitter(0.009) sla_
map=0x3
Seq(2 tunnel-2): state(alive), packet-loss(0.000%) latency(0.030), jitter(0.005) sla_
map=0x3
Seq(2 tunnel-2_0): state(alive), packet-loss(0.000%) latency(0.031), jitter(0.004) sla_
map=0x3
```

## SD-WAN GUI and monitoring enhancements

The SD-WAN pages in the GUI are updated to simplify SD-WAN configuration. New charts and monitoring capabilities are also added. DNS is now a supported protocol in performance SLA.

### SD-WAN interfaces

The SD-WAN interface list shows pie charts at the top of the list, and includes more information about each interface in the table, such as the number of sessions and the bytes sent and received.



The gateway configuration for an SD-WAN interface that is using DHCP is simplified.

### SD-WAN rules

In the SD-WAN rules list, the interface that is currently selected by the rule has a checkmark next to its name in the *Members* column. Hover the cursor over the checkmark to open a tooltip that gives the reason why that member is

selected, such as *has best measured performance*. Even if multiple members are selected, only the highest ranked member is highlighted, unless the mode is *Maximize Bandwidth (SLA)* (load-balance).

*Hit Count* and *Last Used* columns are also added to the table.

ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used	Performance SLA	Status	Port	Protocol
1	Finance		10.100.20.0	Latency	port12 To_VLAN_30 (port9) To_Juniper_ge-0/0/2 (port13)	0	48 seconds ago	Default_DNS	Enabled	any	any
2	balance		10.100.20.0	SLA	port12 To_VLAN_30 (port9) To_Juniper_ge-0/0/2 (port13)	0	48 seconds ago	ping	Enabled	any	any
3	sla		10.100.21.0	SLA	port12 To_VLAN_30 (port9) To_Juniper_ge-0/0/2 (port13)	0	48 seconds ago	ping	Enabled	any	any
4	manual		Act-on-LDAP Act-on-NetBIOS.Name.Service AutoDesk.360		port12	0	48 seconds ago		Enabled	any	any

Hover over a member name to open the SD-WAN member tooltip. It includes health check and SLA statistics tables.

ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used	Performance SLA	Status	Port	Protocol
1	Finance		10.100.20.0	Latency	port12 To_VLAN_30 (port9) To_Juniper_ge-0/0/2 (port13)	95,838	2 seconds ago	Default_DNS	Enabled	any	any
2	balance		10.100.20.0	SLA	port12 To_VLAN_30 (port9) To_Juniper_ge-0/0/2 (port13)	0	48 seconds ago	ping	Enabled	any	any
3	sla		10.100.21.0	SLA	port12 To_VLAN_30 (port9) To_Juniper_ge-0/0/2 (port13)	0	48 seconds ago	ping	Enabled	any	any
4	manual		Act-on-LDAP Act-on-NetBIOS.Name.Service AutoDesk.360		port12				Enabled	any	any

port12

Interface: To\_VLAN\_30 (port9)

Link: 100 Mbps / Full Duplex

Type: Physical Interface

IPv4 Addresses: 172.16.200.1/24

SD-WAN Bandwidth: 1.28 Mbps

SD-WAN Upstream Bandwidth Utilization: 100%

SD-WAN Downstream Bandwidth Utilization: 100%

Performance SLA	Packet Loss	Latency	Jitter
Default_DNS	0.00%	0.57ms	0.05ms
Target 1	5.00%	250.00ms	50.00ms

When editing an SD-WAN rule, the strategies are listed on cards that include a brief description of that strategy. The gutter on the right side of the page includes the hit count for the rule, when it was last used, and a table showing statistics for the currently selected interfaces and SLA targets (depending on the selected strategy).

**FortiGate VM64** FortiGate-VM64

**SD-WAN Rules**

**Rule Name:** balance

**Source:**

- Source address: 10.100.20.0
- User group: +

**Destination:**

- Address: 10.100.20.0
- Protocol number: TCP UDP **ANY** Specify 0
- Internet Service: +
- Application: +

**Outgoing Interfaces:**

- ☒ **Manual**  
Manually assign outgoing interfaces.
- ☐ **Best Quality**  
The interface with the best measured performance is selected.
- ☐ **Lowest Cost (SLA)**  
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.
- ☒ **Maximize Bandwidth (SLA)**  
Traffic is load balanced among interfaces that meet SLA targets.

**Interface preference:**

- port12
- To\_VLAN\_30 (port9)
- To\_Juniper\_ge-0/0/2 (port13)

**Required SLA target:** ping

**Status:** ☒ Enable ☐ Disable

**SLA Details:**

	Packet Loss	Latency	Jitter
ping	0.00%	5.00ms	5.00ms
port12	0.00%	0.24ms	0.02ms
To_VLAN_30 (port9)	?	?	?
To_Juniper_ge-0/0/2 (port13)	0.00%	0.70ms	0.10ms

**Documentation:**

- Online Help
- Video Tutorials

When *Manual* mode is selected, multiple members can be selected.

**FortiGate VM64** FortiGate-VM64

**SD-WAN Rules**

**Rule Name:** manual

**Source:**

- Source address: +
- User group: +

**Destination:**

- Address: +

**Internet Service:**

- Act-on-LDAP
- Act-on-NetBIOS.Name.Service

**Application:**

- AutoDesk.360

**Outgoing Interfaces:**

- ☒ **Manual**  
Manually assign outgoing interfaces.
- ☐ **Best Quality**  
The interface with the best measured performance is selected.
- ☐ **Lowest Cost (SLA)**  
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.
- ☐ **Maximize Bandwidth (SLA)**  
Traffic is load balanced among interfaces that meet SLA targets.

**Interface preference:**

- port12
- To\_VLAN\_30 (port9)
- To\_Juniper\_ge-0/0/2 (port13)

**Status:** ☒ Enable ☐ Disable

**Select Entries Dialog:**

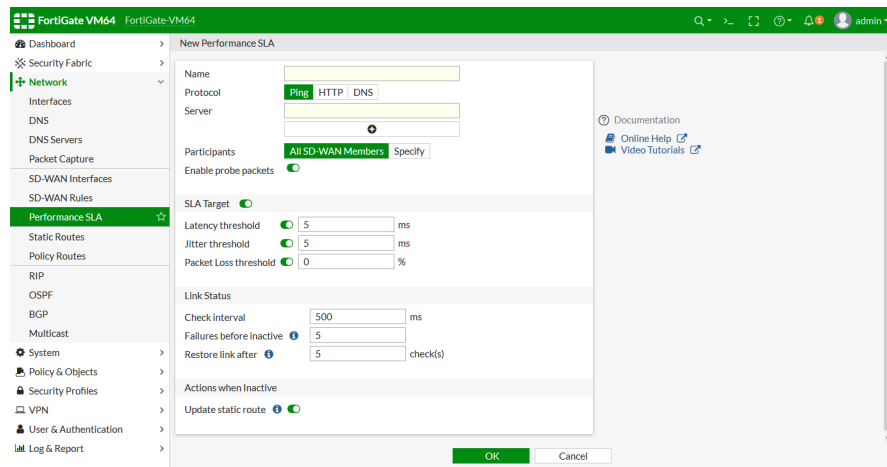
- Search: +
- port12
- To\_VLAN\_30 (port9)
- To\_Juniper\_ge-0/0/2 (port13)

**Close**

## Performance SLA

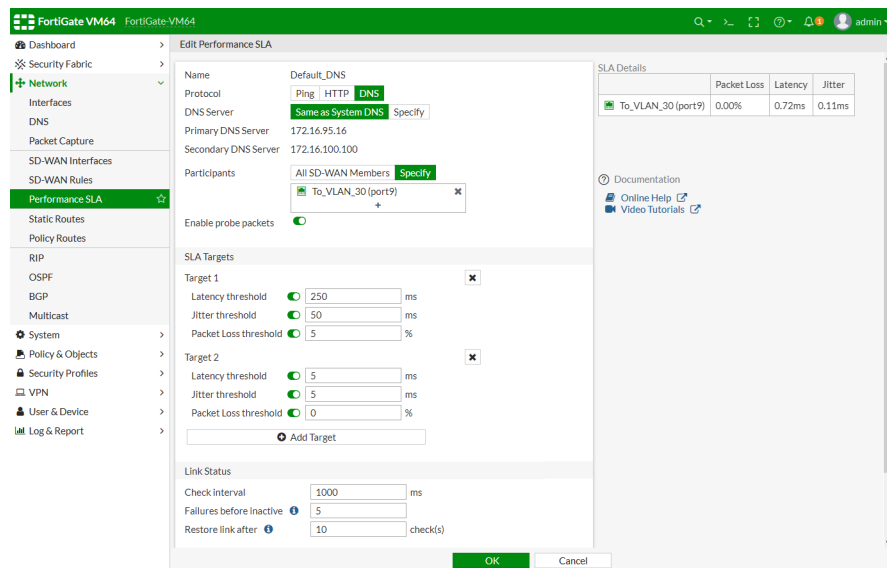
### SLA targets

When configuring a performance SLA, by default, only one SLA target can be configured. Additional targets can be created in the CLI, after which they will also be available from the GUI.



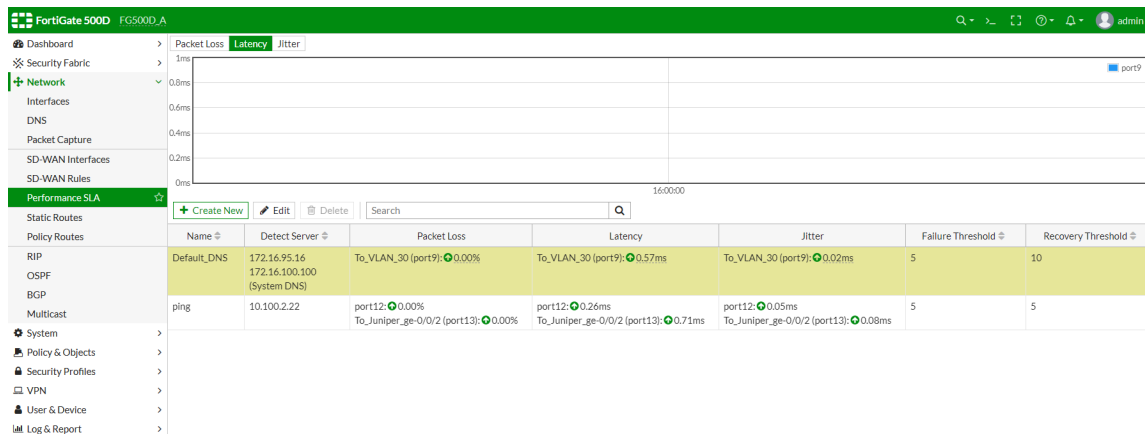
### DNS protocol

The IPv4 DNS protocol can be selected, and the system DNS servers can be used.



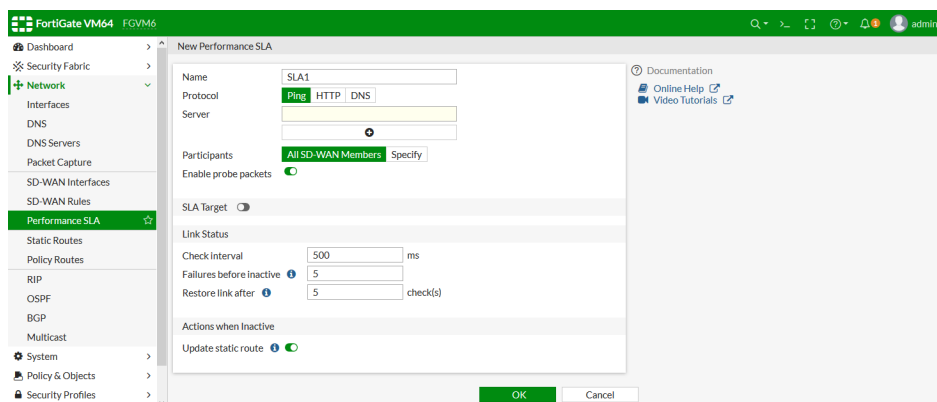
In the Performance SLA table, the *Detect Server* column will show that the system DNS servers are used.





## Participants

When adding a new performance SLA, by default, all SD-WAN members are included as participants.



In the CLI, `member` is set to zero to include all participants.

```
config system virtual-wan-link
  config health-check
    edit "SLA1"
      set system-dns enable
      set members 0
    next
  end
end
```

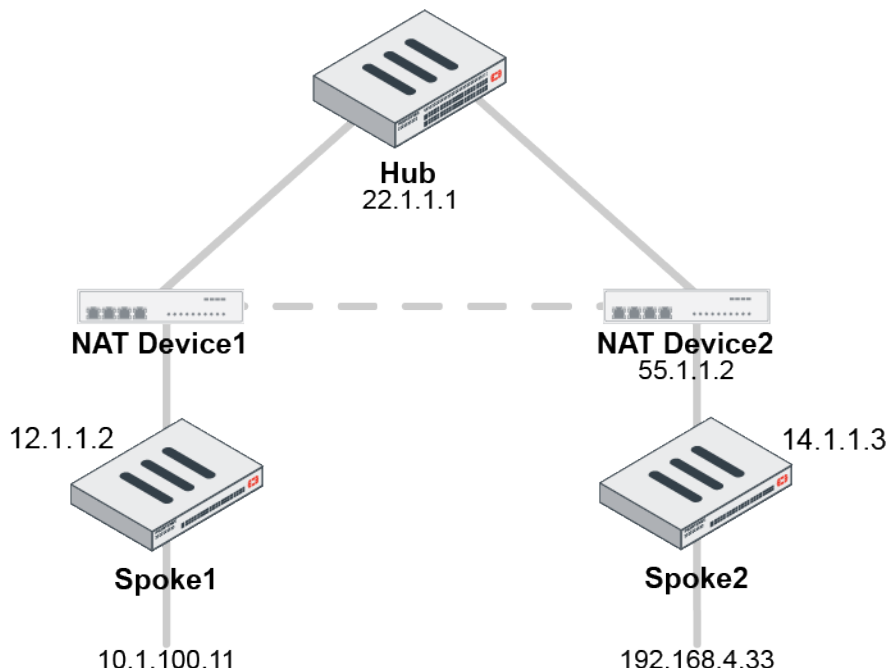
## Routing monitor

*Hit Count* and *Last Used* columns are added to the *Network > Policy Routes* page and *Policy Routing* widget.

## Enhance ADVPN to support UDP hole punching for spokes behind NAT

Previously, spokes behind NAT devices could only create shortcuts if DNAT was used on the NAT devices. This feature adds UDP hole punching capability, which allows ADVPN shortcuts to be established through a UDP hole on a NAT device. The NAT device must support RFC 4787 Endpoint-Independent Mapping.

In the following example, device 10.1.100.11 behind Spoke1 needs to reach device 192.168.4.33 behind Spoke2. Spoke1 and Spoke2 are behind NAT devices and have established IPsec tunnels to the Hub. The hole punching creates a shortcut between Spoke1 and Spoke2 that bypasses the Hub.



To verify the ADVPN shortcut is established between both spokes behind NAT:

```

# diagnose debug enable
# diagnose debug application ike -1
ike 0: comes 22.1.1.1:4500->12.1.1.2:4500,ifindex=6....
ike 0: IKEv1 exchange=Informational id=3c10fb6a76f1e264/6c7b397100dffc63:58ac7c02 len=204
ike 0:toHub1:35: notify msg received: SHORTCUT-OFFER
ike 0:toHub1: shortcut-offer 10.1.100.11->192.168.4.33 psk 64 ppk 0 ver 1 mode 0
ike 0 looking up shortcut by addr 192.168.4.33, name toHub1
ike 0:toHub1: send shortcut-query 1438189781753480593 d3fdd1bfb94caee/0000000000000000
12.1.1.2 10.1.100.11->192.168.4.33 psk 64 ttl 32 nat 1 ver 1 mode 0
ike 0:toHub1:35: sent IKE msg (SHORTCUT-QUERY): 12.1.1.2:4500->22.1.1.1:4500, len=236,
id=3c10fb6a76f1e264/6c7b397100dffc63:12e263f7
ike 0: comes 22.1.1.1:4500->12.1.1.2:4500,ifindex=6....
ike 0: IKEv1 exchange=Informational id=3c10fb6a76f1e264/6c7b397100dffc63:4976e1ac len=236
ike 0:toHub1:35: notify msg received: SHORTCUT-REPLY
ike 0:toHub1: rcv shortcut-reply 1438189781753480593 d3fdd1bfb94caee/16a1eb5b0f37ee23
14.1.1.3 to 10.1.100.11 psk 64 ppk 0 ver 1 mode 0 nat 55.1.1.2:64916
ike 0:toHub1: iif 22 192.168.4.33->10.1.100.11 route lookup oif 21
ike 0:toHub1: shortcut-reply received from 55.1.1.2:64916, local-nat=yes, peer-nat=yes
ike 0:toHub1: NAT hole punching to peer at 55.1.1.2:64916
ike 0:toHub1: created connection: 0x5e71f58 6 12.1.1.2->55.1.1.2:64916.
<==55.1.1.2:64916 this is UDP hole of NAT device
ike 0:toHub1: adding new dynamic tunnel for 55.1.1.2:64916
ike 0:toHub1_0: added new dynamic tunnel for 55.1.1.2:64916
ike 0:toHub1_0:48: initiator: main mode is sending 1st message...
ike 0:toHub1_0:48: cookie d3fdd1bfb94caee/16a1eb5b0f37ee23
ike 0:toHub1_0:48: sent IKE msg (ident_i1send): 12.1.1.2:4500->55.1.1.2:64916, len=632,
id=d3fdd1bfb94caee/16a1eb5b0f37ee23
  
```

```
ike 0: comes 55.1.1.2:64916->12.1.1.2:4500,ifindex=6....
ike 0: IKEv1 exchange=Identity Protection id=d3fdd1bfbc94caee/16aleb5b0f37ee23 len=252
ike 0:toHub1_0:48: initiator: main mode get 1st response...
...
ike 0:toHub1_0:48: negotiation result
ike 0:toHub1_0:48: proposal id = 1:
ike 0:toHub1_0:48:   protocol id = ISAKMP:
ike 0:toHub1_0:48:   trans_id = KEY_IKE.
ike 0:toHub1_0:48:   encapsulation = IKE/none
ike 0:toHub1_0:48:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:toHub1_0:48:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:toHub1_0:48:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:toHub1_0:48:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:toHub1_0:48: ISAKMP SA lifetime=86400
ike 0:toHub1_0:48: sent IKE msg (ident_i2send): 12.1.1.2:4500->55.1.1.2:64916, len=380,
id=d3fdd1bfbc94caee/16aleb5b0f37ee23
ike 0: comes 55.1.1.2:64916->12.1.1.2:4500,ifindex=6....
ike 0: IKEv1 exchange=Identity Protection id=d3fdd1bfbc94caee/16aleb5b0f37ee23 len=380
ike 0:toHub1_0:48: initiator: main mode get 2nd response...
...
ike 0:toHub1_0:48: add INITIAL-CONTACT
ike 0:toHub1_0:48: add INTERFACE-ADDR4 10.10.1.100
ike 0:toHub1_0:48: sent IKE msg (ident_i3send): 12.1.1.2:4500->55.1.1.2:64916, len=140,
id=d3fdd1bfbc94caee/16aleb5b0f37ee23
ike 0: comes 55.1.1.2:64916->12.1.1.2:4500,ifindex=6....
ike 0: IKEv1 exchange=Identity Protection id=d3fdd1bfbc94caee/16aleb5b0f37ee23 len=124
ike 0:toHub1_0:48: initiator: main mode get 3rd response...
ike 0:toHub1_0:48: received pl notify type INTERFACE-ADDR4
ike 0:toHub1_0:48: INTERFACE-ADDR4 10.10.1.102
ike 0:toHub1_0:48: peer identifier IPV4_ADDR 14.1.1.3
ike 0:toHub1_0:48: PSK authentication succeeded
ike 0:toHub1_0:48: authentication OK
ike 0:toHub1_0:48: established IKE SA d3fdd1bfbc94caee/16aleb5b0f37ee23
ike 0:toHub1_0:48: auto-discovery receiver
ike 0:toHub1_0:48: auto-discovery 2
ike 0:toHub1_0: add R/32 route 10.10.1.102 via 10.10.1.102, intf=toHub1(22)
ike 0:toHub1_0: add peer route 10.10.1.102
ike 0:toHub1: schedule auto-negotiate
ike 0:toHub1_0:48: no pending Quick-Mode negotiations
ike 0:toHub1_0:toHub1: IPsec SA connect 6 12.1.1.2->55.1.1.2:64916
ike 0:toHub1_0:toHub1: using existing connection
ike 0:toHub1_0:toHub1: traffic triggered, serial=1 1:10.1.100.11:2048->1:192.168.4.33:0
ike 0:toHub1:toHub1: config found
ike 0:toHub1_0:toHub1: IPsec SA connect 6 12.1.1.2->55.1.1.2:64916 negotiating
ike 0:toHub1_0:48: cookie d3fdd1bfbc94caee/16aleb5b0f37ee23:8465e467
ike 0:toHub1_0:48:toHub1:109: natt flags 0x1f, encmode 1->3
ike 0:toHub1_0:48:toHub1:109: initiator selectors 0 0:0.0.0.0/0.0.0.0:0-
>0:0.0.0.0/0.0.0.0:0
ike 0:toHub1_0:48: sent IKE msg (quick_i1send): 12.1.1.2:4500->55.1.1.2:64916, len=620,
id=d3fdd1bfbc94caee/16aleb5b0f37ee23:8465e467
ike 0: comes 55.1.1.2:64916->12.1.1.2:4500,ifindex=6....
ike 0: IKEv1 exchange=Quick id=d3fdd1bfbc94caee/16aleb5b0f37ee23:8465e467 len=444
ike 0:toHub1_0:48:toHub1:109: responder selectors 0:0.0.0.0/0.0.0.0:0->0:0.0.0.0/0.0.0.0:0
ike 0:toHub1_0:48:toHub1:109: my proposal:
```

```
...
...
ike 0:toHub1_0:48:toHub1:109: add IPsec SA: SPIs=79654cf1/5e9936a5
ike 0:toHub1_0:48:toHub1:109: IPsec SA dec spi 79654cf1 key
16:5E21180992B8892DE5142E1F53ABD29E auth 20:49AA4AE14994A39A138392AC517B6E79D98CA673
ike 0:toHub1_0:48:toHub1:109: IPsec SA enc spi 5e9936a5 key
16:BE16B8EF4E75F7B3CF97A1D58D996890 auth 20:2F46B57CAC6F3185BB182F9280312263325F6BAF
ike 0:toHub1_0:48:toHub1:109: added IPsec SA: SPIs=79654cf1/5e9936a5
ike 0:toHub1_0:48:toHub1:109: sending SNMP tunnel UP trapp
```

### To verify the spoke-to-spoke IPsec phase 1 tunnel shortcut is established:

```
# diagnose vpn ike gateway list
vd: root/0
name: toHub1
version: 1
interface: wan2 6
addr: 12.1.1.2:4500 -> 22.1.1.1:4500
created: 503s ago
assigned IPv4 address: 10.10.1.100/255.255.255.0
nat: me
auto-discovery: 2 receiver
IKE SA: created 1/1 established 1/1 time 0/0/0 ms
IPsec SA: created 1/3 established 1/3 time 0/0/0 ms

id/spi: 35 3c10fb6a76f1e264/6c7b397100dffc63
direction: initiator
status: established 503-503s ago = 0ms
proposal: aes128-sha256
key: 7fca86063ea2e72f-4efea6f1bec23948
lifetime/rekey: 86400/85596
DPD sent/recv: 00000000/00000000

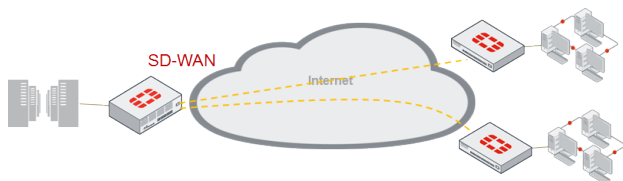
vd: root/0
name: toHub1_0
version: 1
interface: wan2 6
addr: 12.1.1.2:4500 -> 55.1.1.2:64916
created: 208s ago
nat: me peer
auto-discovery: 2 receiver
IKE SA: created 1/1 established 1/1 time 20/20/20 ms
IPsec SA: created 1/1 established 1/1 time 10/10/10 ms

id/spi: 48 d3fdd1bfbc94caee/16a1eb5b0f37ee23
direction: initiator
status: established 208-208s ago = 20ms
proposal: aes128-sha256
key: 9bcac400d8e14e11-fffde33eaa3a8263
lifetime/rekey: 86400/85891
DPD sent/recv: 0000000a/00000000
```

## SD-WAN health check packet enhancement

SD-WAN health check probe packets now support Differentiated Services Code Point (DSCP) markers for accurate evaluation of the link performance for high priority applications by upstream devices.

When the SD-WAN health check packet is sent out, the DSCP can be set with a CLI command.



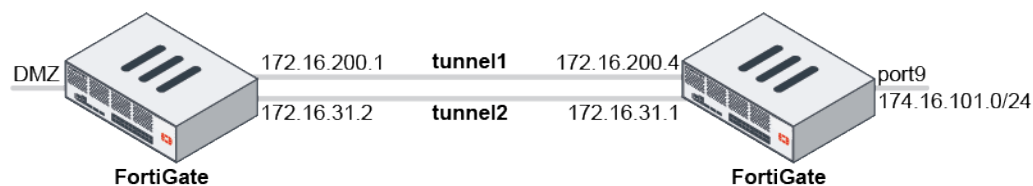
### To mark health-check packets with DSCP:

```
config system virtual-wan-link
  config health-check
    edit <name>
      set diffservcode <6 bits binary, range 000000-111111>
    next
  end
end
```

## Weighted round robin for IPsec aggregate tunnels

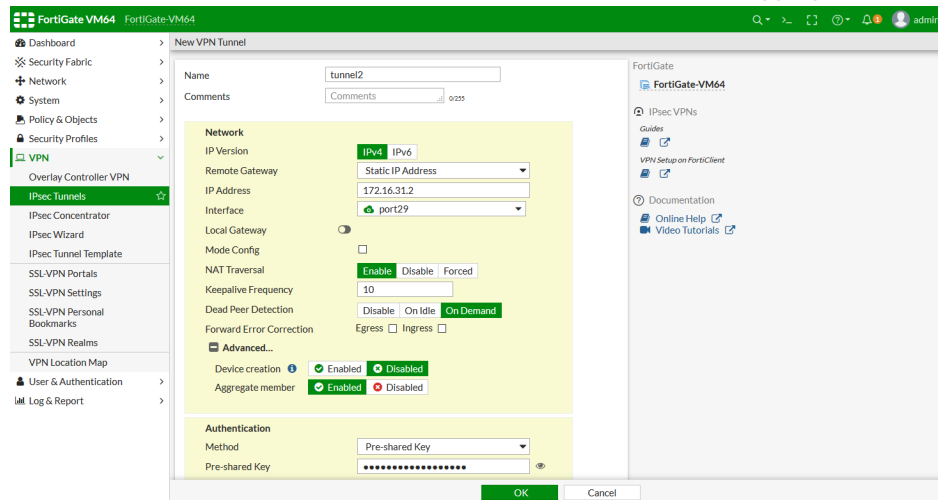
A weighted round robin algorithm can be used for IPsec aggregate tunnels to distribute traffic by the weight of each member tunnel.

In this example, the FortiGate has two IPsec tunnels put into IPsec aggregate. Traffic is distributed among the members, with one third over *tunnel1*, and two thirds over *tunnel2*. To achieve this, the weighted round robin algorithm is selected, *tunnel1* is assigned a weight of 10, and *tunnel2* is assigned a weight of 20.

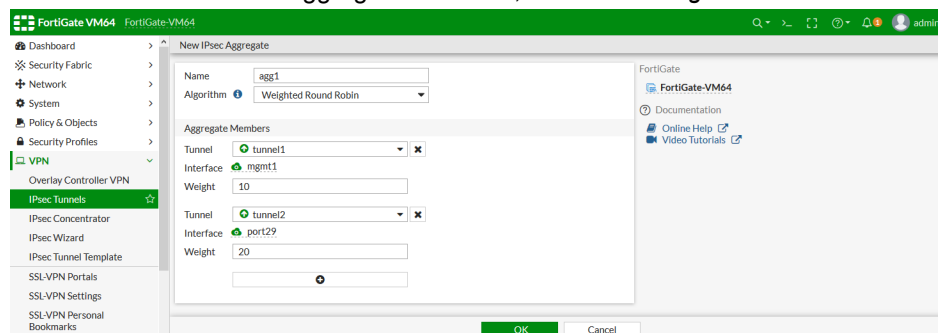


## To create the IPsec aggregate in the GUI:

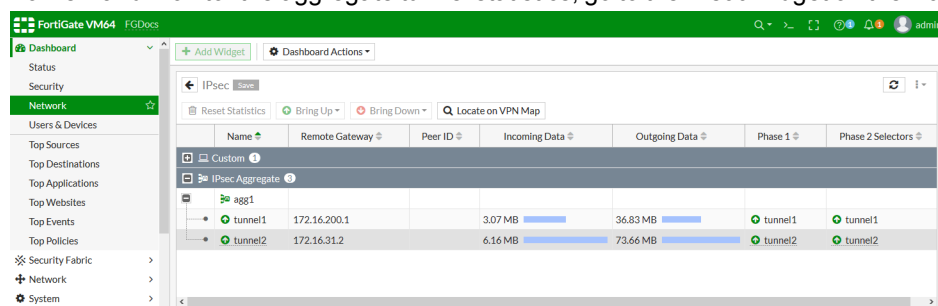
1. Create the *tunnel1* and *tunnel2* custom IPsec tunnels. Ensure that *Aggregate member* is *Enabled* for each tunnel.



2. Go to *VPN > IPsec Tunnels* and click *Create New > IPsec Aggregate*.
3. Enter a name for the aggregate, such as *agg1*, and ensure that *Algorithm* is *Weighted Round Robin*.
4. Add *tunnel1* as an aggregate members, and set *Weight* to 10.
5. Add *tunnel2* as a second aggregate members, and set its *Weight* to 20.



6. Click *OK*.
7. To view and monitor the aggregate tunnel statistics, go to the *IPsec* widget on the *Network* dashboard.



## To create the IPsec aggregate in the CLI:

1. Create the *tunnel1* and *tunnel2* custom IPsec tunnels with aggregate-member enabled and aggregate-weight set for both tunnels:

```

config vpn ipsec phase1-interface
edit "tunnell1"
...
set aggregate-member enable
set aggregate-weight 10
...
next
edit "tunnel2"
...
set aggregate-member enable
set aggregate-weight 20
...
next
end

```

## 2. Create the IPsec aggregate:

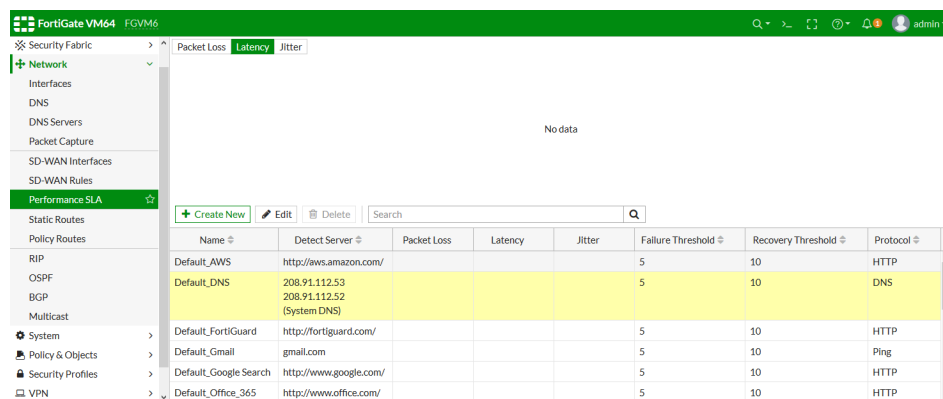
```

config system ipsec-aggregate
edit "agg1"
set member "tunnell1" "tunnel2"
set algorithm weighted-round-robin
next
end

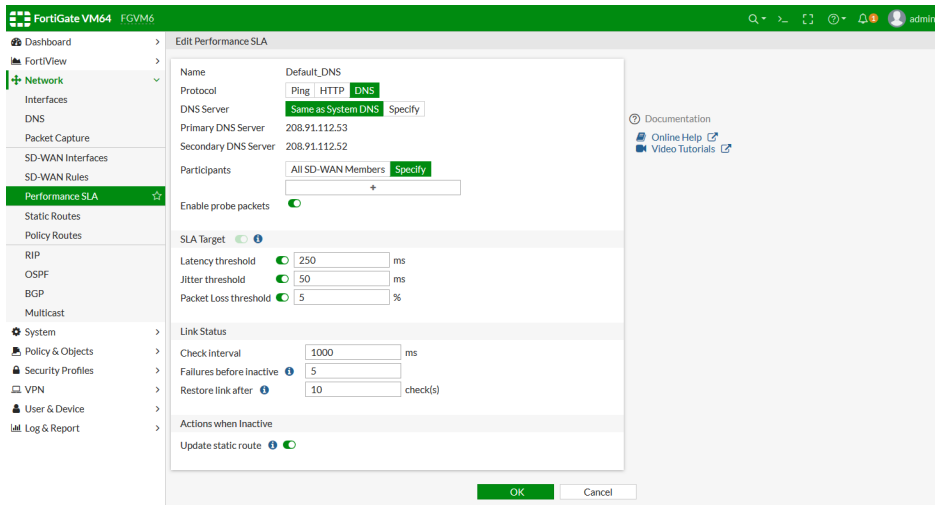
```

## Default\_DNS performance SLA profile

A new Default\_DNS performance SLA is added after performing a factory reset.



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold	Protocol
Default_AWS	http://aws.amazon.com/				5	10	HTTP
Default_DNS	208.91.112.53 208.91.112.52 (System DNS)				5	10	DNS
Default_FortiGuard	http://fortiguard.com/				5	10	HTTP
Default_Gmail	gmail.com				5	10	Ping
Default_Google Search	http://www.google.com/				5	10	HTTP
Default_Office_365	http://www.office.com/				5	10	HTTP

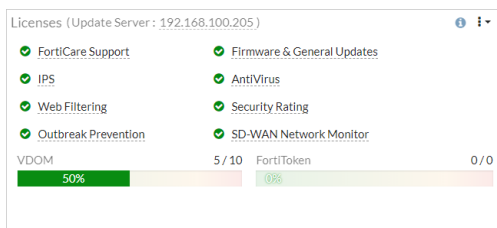


```
config system virtual-wan-link
config health-check
edit "Default_DNS"
set system-dns enable
set interval 1000
set probe-timeout 1000
set recoverytime 10
config sla
edit 1
set latency-threshold 250
set jitter-threshold 50
set packetloss-threshold 5
next
end
next
end
end
```

## Interface speedtest

An interface speedtest can be performed on WAN interfaces in the GUI. The results of the test can be added to the interface's *Estimated bandwidth*. An SD-WAN Network Monitor license is required.

The *License* widget and the *System > FortiGuard* page display the SD-WAN Network Monitor license status.





FortiGuard Distribution Network

Entitlement	Status
FortiCare Support	Registered - stephenzhang@fortinet.com <a href="#">Launch Portal</a>
Hardware Version	Advanced hardware - expires on 2022/05/06
Enhanced Support	24x7 support - expires on 2022/05/06
Firmware & General Updates	Licensed - expires on 2022/05/06
Application Control Signatures	Version 15.00792 <a href="#">Upgrade Database</a> <a href="#">View List</a>
Device & OS Identification	Version 1.00093
Internet Service Database Definitions	Version 7.00518
Intrusion Prevention	Licensed - expires on 2022/05/06
IPS Definitions	Version 15.00792 <a href="#">Upgrade Database</a> <a href="#">View List</a>
IPS Engine	Version 6.00011
Malicious URLs	Version 2.00578 <a href="#">View List</a>
Botnet IPs	Version 4.00631 <a href="#">View List</a>
Botnet Domains	Version 2.00447 <a href="#">View List</a>
AntiVirus	Licensed - expires on 2022/05/06
AV Definitions	Version 75.01821 <a href="#">Upgrade Database</a>
AV Engine	Version 6.00144
Mobile Malware	Version 75.01845
SD-WAN Network Monitor	Licensed - expires on 2022/03/11
Outbreak Prevention	Licensed - expires on 2022/05/06
Industrial DB	Licensed - expires on 2022/03/11
Industrial Attack Definitions	Version 15.00791

Apply

FortiGate  
FGT\_A

Fortinet Service Communications

Service	Traffic Volume (Last 24 hours)
FortiCare	0 B
FortiCloud Log	0 B
FortiGuard.com	1.07 MB
FortiGuard Download	24.35 MB
FortiGuard Query	15.24 kB
FortiSandbox Cloud	0 B
OCVPN	1.47 kB
SDNS	0 B
FortiToken Registration	0 B
SMS Service	0 B

Documentation  
[Online Help](#)  
[Video Tutorials](#)  
[How to Purchase/Renew Fortinet Service Subscriptions](#)

## To run an interface speedtest in the GUI:

1. Go to **Network > Interfaces**.
2. Edit a WAN interface. The interfaces can be grouped by role using the grouping dropdown on the right side of the toolbar.
3. Click **Execute speed test** in the right pane.

Edit Interface

Name: To\_VLAN\_30 (port19)  
Alias: To\_VLAN\_30  
Type: Physical Interface  
Virtual domain: root  
Role: WAN  
Estimated bandwidth: 0 kbps Upstream, 0 kbps Downstream

Address  
Addressing mode: Manual DHCP  
IP/Netmask: 172.16.200.1/255.255.255.0  
IPv6 addressing mode: Manual DHCP  
IPv6 Address/Prefix: ::0  
Secondary IP address: +

Administrative access  
IPv4: ☒ HTTPS ☒ HTTP ☒ PING ☒ SNMP  
☒ Telnet ☐ SSH ☐ FTN ☐ RADIUS Accounting  
☐ Security Fabric Connection  
IPv6: ☐ HTTPS ☐ PING ☐ FMG-Access  
☐ SSH ☐ SNMP ☐ Security Fabric Connection  
Receive LLDP: Use VDOM Setting [Enable](#) [Disable](#)  
Transmit LLDP: Use VDOM Setting [Enable](#) [Disable](#)

Traffic Shaping  
Outbound shaping profile: +

Miscellaneous

OK Cancel

FortiGate  
FGT\_A

Active Administrator Sessions  
HTTPS

Status  
Up

MAC address  
90:6c:ac:88:4d:93

Speed Test  
Upstream: 41.13 Mbps  
Downstream: 81.17 Mbps  
Measured on: 2020/03/08 12:36:12

[Execute speed test](#)  
[Apply results to estimated bandwidth](#)

Documentation  
[Online Help](#)  
[Video Tutorials](#)

4. When the test completes, click *Apply results to estimated bandwidth*.

The speedtest results are used to populate the *Estimated bandwidth* fields.

5. Click **OK**.

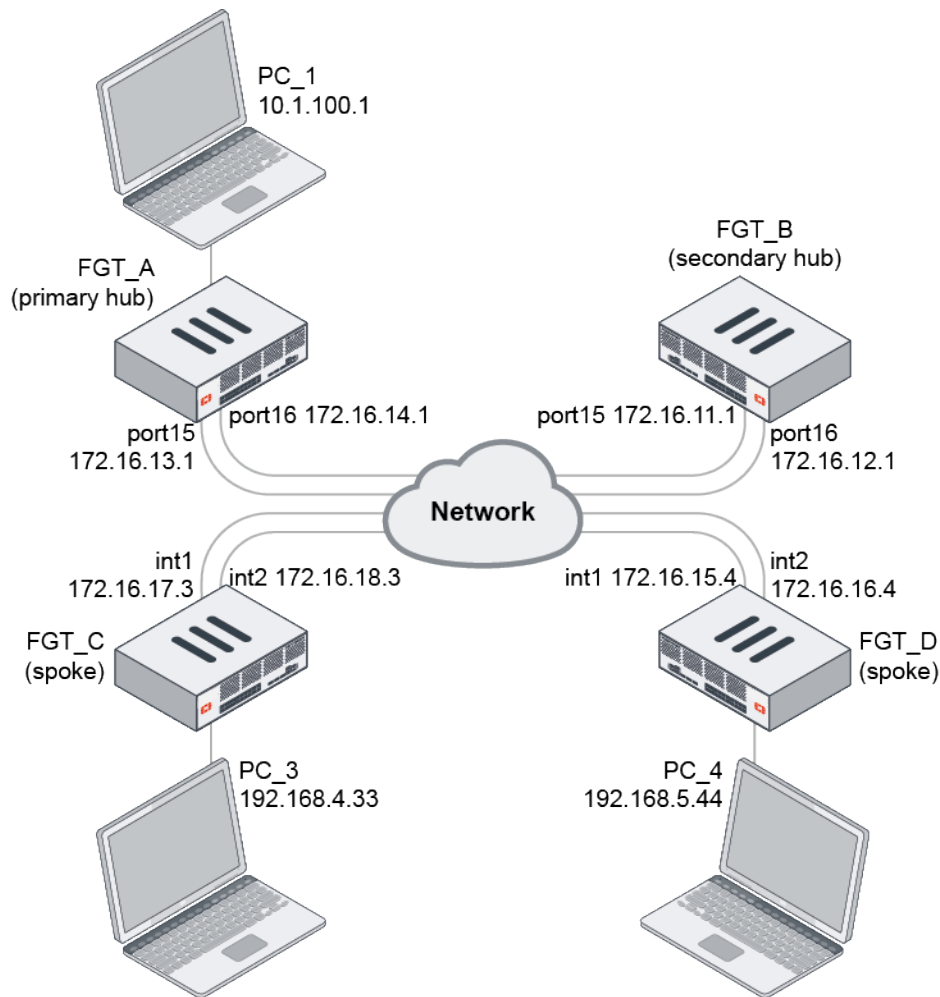


The FortiGate must be connected to FortiGuard, and able to reach either the AWS or Google speedtest servers.

## Support SD-WAN integration with OCVPN

OCVPN now has the capability to enable SD-WAN in order to dynamically add its tunnel interfaces as SD-WAN members. Users can configure SD-WAN health checks and service rules to direct traffic over the OCVPN tunnels.

The following example uses a dual hub and spoke topology. Each hub and spoke has two WAN link connections to the ISP. The spokes generate two IPsec tunnels to each hub (four tunnels in total). BGP neighbors are established over each tunnel and routes from the hubs and other spokes learned from all neighbors, which forms an ECMP scenario. All tunnels are placed as SD-WAN members, so traffic can be distributed across tunnels based on the configured SD-WAN service rules.



### To integrate SD-WAN with OCVPN in the GUI:

1. Configure the primary hub:
  - a. Go to *VPN > Overlay Controller VPN* and set the *Status* to *Enable*.
  - b. For *Role*, select *Primary Hub*.
  - c. Enter the WAN interfaces (*port15* and *port16*) and tunnel IP allocation block (*10.254.0.0/16*).



The WAN interface is position sensitive, meaning a tunnel will be created with the first position interface on the hub to the first position interface on the spoke, and so on. In this example, FGT\_A (primary hub) will create two tunnels with FGT\_C (spoke):

- FGT\_A port15 <==> FGT\_C internal1
- FGT\_A port16 <==> FGT\_C internal2

- d. Enable *Auto-discovery shortcuts*.
- e. Enable *Add OCVPN tunnels to SD-WAN*. The IPsec tunnels will be added automatically to the SD-WAN members if SD-WAN is enabled.

## 2. Configure the overlays on the primary hub:

- a. In the *Overlays* section, click *Create New*.
- b. Enter a name and add the local interface (*port2*). Note the overlay is either based on local subnets or local interfaces, but not both.

By default, inter-overlay traffic is not enabled. Toggle *Allow traffic from other overlays* to enable it.

- c. Click *OK* and repeat these steps to create the second overlay (*loop1*).

- d. Click *Apply*.

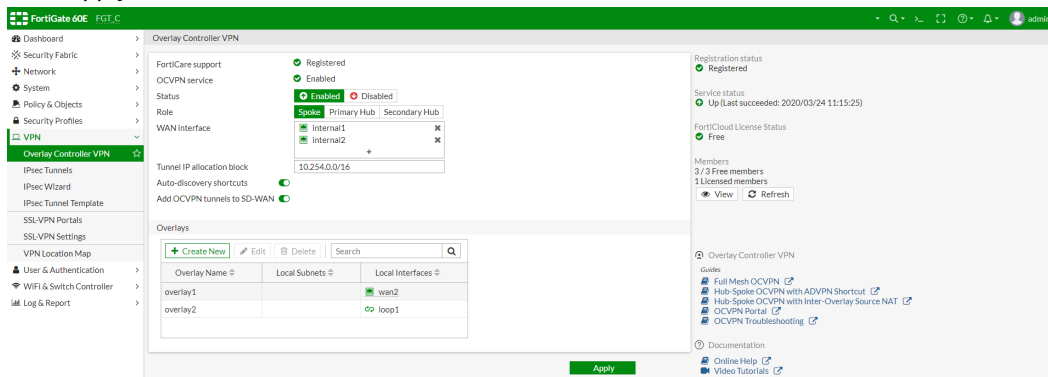
## 3. Configure the secondary hub with the same settings as the primary hub.

## 4. Configure the spoke:

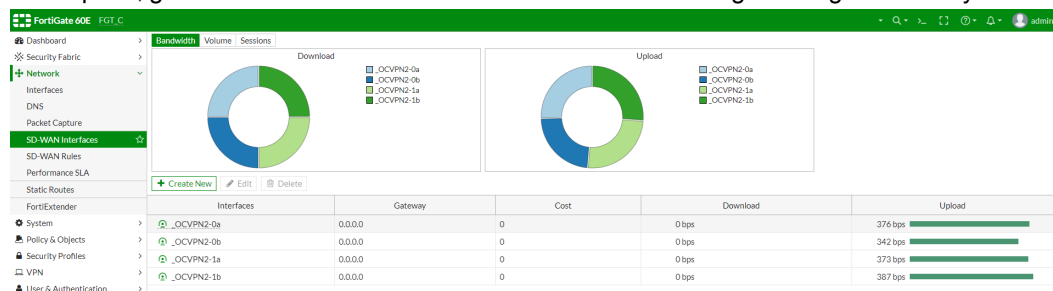
- a. Go to *VPN > Overlay Controller VPN* and set the *Status* to *Enable*.
- b. For *Role*, select *Spoke*.
- c. Enter the WAN interfaces (*internal1* and *internal2*).
- d. Enable *Auto-discovery shortcuts*.
- e. Enable *Add OVPN tunnels to SD-WAN*. The IPsec tunnels will be added automatically to the SD-WAN members if SD-WAN is enabled.
- f. Configure the overlays.



The overlay names on the spokes must match the hub for the traffic to be allowed through the same overlay.

g. Click *Apply*.

## 5. Configure the other spoke with the same settings.

6. On a spoke, go to *Network > SD-WAN Interfaces* to view the configuration generated by OCVPN.

Firewall policies will be automatically generated by OCVPN between the local interfaces and the SD-WAN interface. Each policy will define the proper local and remote networks for its source and destination addresses.

**To integrate SD-WAN with OCVPN in the CLI:**

## 1. Configure the primary hub:

```
config vpn ocvpn
  set role primary-hub
  set sdwan enable
  set wan-interface "port15" "port16"
  set ip-allocation-block 10.254.0.0 255.255.0.0
  config overlays
    edit "overlay1"
      config subnets
        edit 1
          set type interface
          set interface "port2"
        next
      end
    next
    edit "overlay2"
      config subnets
        edit 1
          set type interface
          set interface "loop1"
        next
      end
    next
  end
end
```

```

    end
end

```

**2. Configure the secondary hub with the same settings as the primary hub.**

**3. Configure the spoke:**

```

config vpn ocvpn
    set status enable
    set sdwan enable
    set wan-interface "internal1" "internal2"
    config overlays
        edit "overlay1"
            config subnets
                edit 1
                    set type interface
                    set interface "wan2"
                next
            end
        next
        edit "overlay2"
            config subnets
                edit 1
                    set type interface
                    set interface "loop1"
                next
            end
        next
    end
end

```

**4. Configure the other spoke with the same settings.**

**5. Configure SD-WAN:**

```

config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "_OCVPN2-0a"
        next
        edit 2
            set interface "_OCVPN2-0b"
        next
        edit 3
            set interface "_OCVPN2-1a"
        next
        edit 4
            set interface "_OCVPN2-1b"
        next
    end
end

```

Firewall policies will be automatically generated by OCVPN between the local interfaces and the SD-WAN interface. Each policy will define the proper local and remote networks for its source and destination addresses.

## To verify the integration is working after the ADVPN shortcut is triggered:

### 1. Check the routing table on the spoke:

```
FGT_C # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
```

Routing table for VRF=0

```
S*      0.0.0.0/0 [10/0] via 172.16.17.2, internal1
        [10/0] via 172.16.18.2, internal2
B       10.1.100.0/24 [200/0] via 10.254.7.254, _OCVPN2-0a, 00:10:24
        [200/0] via 10.254.15.254, _OCVPN2-0b, 00:10:24
B       10.1.200.0/24 [200/0] via 10.254.7.254, _OCVPN2-0a, 00:10:24
        [200/0] via 10.254.15.254, _OCVPN2-0b, 00:10:24
B       10.2.100.0/24 [200/0] via 10.254.71.254, _OCVPN2-1a, 00:10:15
        [200/0] via 10.254.79.254, _OCVPN2-1b, 00:10:15
B       10.2.200.0/24 [200/0] via 10.254.71.254, _OCVPN2-1a, 00:10:15
        [200/0] via 10.254.79.254, _OCVPN2-1b, 00:10:15
B       10.254.0.0/16 [200/0] via 10.254.7.254, _OCVPN2-0a, 00:10:15
        [200/0] via 10.254.15.254, _OCVPN2-0b, 00:10:15
        [200/0] via 10.254.71.254, _OCVPN2-1a, 00:10:15
        [200/0] via 10.254.79.254, _OCVPN2-1b, 00:10:15
C       10.254.0.0/21 is directly connected, _OCVPN2-0a
C       10.254.0.1/32 is directly connected, _OCVPN2-0a
C       10.254.8.0/21 is directly connected, _OCVPN2-0b
C       10.254.8.1/32 is directly connected, _OCVPN2-0b
C       10.254.64.0/21 is directly connected, _OCVPN2-1a
C       10.254.64.1/32 is directly connected, _OCVPN2-1b_0 <==shortcut tunnel
C       10.254.64.2/32 is directly connected, _OCVPN2-1a
C       10.254.72.0/21 is directly connected, _OCVPN2-1b
C       10.254.72.2/32 is directly connected, _OCVPN2-1b
        is directly connected, _OCVPN2-1b_0
C       172.16.17.0/24 is directly connected, internal1
C       172.16.18.0/24 is directly connected, internal2
C       172.16.200.0/24 is directly connected, wan1
C       192.168.1.0/24 is directly connected, internal
C       192.168.4.0/24 is directly connected, wan2
B       192.168.5.0/24 [200/0] via 10.254.0.2, _OCVPN2-0a, 00:00:10
        [200/0] via 10.254.8.2, _OCVPN2-0b, 00:00:10
        [200/0] via 10.254.0.2, _OCVPN2-0a, 00:00:10
        [200/0] via 10.254.8.2, _OCVPN2-0b, 00:00:10
        [200/0] via 10.254.64.1, _OCVPN2-1b_0, 00:00:10
        [200/0] via 10.254.72.1, _OCVPN2-1b, 00:00:10
        [200/0] via 10.254.64.1, _OCVPN2-1b_0, 00:00:10
        [200/0] via 10.254.72.1, _OCVPN2-1b, 00:00:10
C       192.168.44.0/24 is directly connected, loop1
B       192.168.55.0/24 [200/0] via 10.254.0.2, _OCVPN2-0a, 00:00:10
        [200/0] via 10.254.8.2, _OCVPN2-0b, 00:00:10
        [200/0] via 10.254.0.2, _OCVPN2-0a, 00:00:10
        [200/0] via 10.254.8.2, _OCVPN2-0b, 00:00:10
        [200/0] via 10.254.64.1, _OCVPN2-1b_0, 00:00:10
        [200/0] via 10.254.72.1, _OCVPN2-1b, 00:00:10
```

```
[200/0] via 10.254.64.1, _OCVPN2-1b_0, 00:00:10
[200/0] via 10.254.72.1, _OCVPN2-1b, 00:00:10
```

## 2. Check the VPN tunnel state:

```
FGT_C # diagnose vpn tunnel list
```

```
list all ipsec tunnel in vd 0
```

```
-----
name=_OCVPN2-1b_0 ver=2 serial=1c 172.16.18.3:0->172.16.15.4:0 dst_mtu=1500
bound_if=9 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/728 options[02d8]=npu
create_dev no-sysctl rgwy-chg frag-rfc accept_traffic=1 overlay_id=4
```

```
parent=_OCVPN2-1b index=0
proxyid_num=1 child_num=0 refcnt=15 ilast=0 olast=0 ad=r/2
stat: rxp=641 txp=1025 rxb=16436 txb=16446
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1b proto=0 sa=1 ref=3 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=42650/0B replaywin=1024
seqno=407 esn=0 replaywin_lastseq=00000280 itn=0 qat=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=43186/43200
dec: spi=90f03d9d esp=aes key=16 6cb33685bbc67d5c85488e0176ecf7b0
ah=sha1 key=20 7d11b3babe62c840bf444b7b1f637b4324722a71
enc: spi=7bc94bda esp=aes key=16 b4d8fc731d411eb24448b4077a5872ca
ah=sha1 key=20 b724064d827304a6d80385ed4914461108b7312f
dec:pkts/bytes=641/16368, enc:pkts/bytes=2053/123426
npu_flag=03 npu_rgwy=172.16.15.4 npu_lgwy=172.16.18.3 npu_selid=1f dec_npuid=1 enc_
npuid=1
```

```
-----
name=_OCVPN2-0a ver=2 serial=18 172.16.17.3:0->172.16.13.1:0 dst_mtu=1500
bound_if=8 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu create_
dev frag-rfc accept_traffic=1 overlay_id=1
```

```
proxyid_num=1 child_num=0 refcnt=20 ilast=0 olast=0 ad=r/2
stat: rxp=1665 txp=2922 rxb=278598 txb=70241
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=7
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0a proto=0 sa=1 ref=4 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=41599/0B replaywin=1024
seqno=890 esn=0 replaywin_lastseq=00000680 itn=0 qat=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=42899/43200
dec: spi=90f03d95 esp=aes key=16 a6ffcc197bb1b46ec745d0b595cdd69a
ah=sha1 key=20 8007c134e41edf282f95daf9c9033d688ef05ccc
enc: spi=a1bf21bf esp=aes key=16 ead05be389b0dec222f969e2f9c46b1d
ah=sha1 key=20 b04105d34d4b0e61b018f2e60591f9b1510783bb
dec:pkts/bytes=1665/278538, enc:pkts/bytes=4237/265074
npu_flag=03 npu_rgwy=172.16.13.1 npu_lgwy=172.16.17.3 npu_selid=1b dec_npuid=1 enc_
npuid=1
```

```
-----
name=_OCVPN2-1a ver=2 serial=1a 172.16.17.3:0->172.16.11.1:0 dst_mtu=1500
bound_if=8 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu create_
dev frag-rfc accept_traffic=1 overlay_id=3
```



```
proxyid_num=1 child_num=0 refcnt=17 ilast=0 olast=0 ad=r/2
stat: rxp=1 txp=2913 rxb=16376 txb=69642
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=5
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1a proto=0 sa=1 ref=28 serial=1 auto-negotiate adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=41653/0B replaywin=1024
    seqno=887 esn=0 replaywin_lastseq=00000002 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42900/43200
  dec: spi=90f03d9b esp=aes key=16 ee03f5b0f617a26c6177e91d60abf90b
    ah=sha1 key=20 f60cbbc4ebbd6d0327d23137da707b7ab2dc49e6
  enc: spi=a543a7d3 esp=aes key=16 1d37efab13a5c0347b582b2198b15cb8
    ah=sha1 key=20 427ee4c82bac6f26f0bcabfe04328c7f57ce682e
  dec:pkts/bytes=1/16316, enc:pkts/bytes=4229/264036
  npu_flag=03 npu_rgw=172.16.11.1 npu_lgw=172.16.17.3 npu_selid=1d dec_npuid=1 enc_
npuid=1
-----
name=_OCVPN2-0b ver=2 serial=19 172.16.18.3:0->172.16.14.1:0 dst_mtu=1500
bound_if=9 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu create_
dev frag-rfc accept_traffic=1 overlay_id=2

proxyid_num=1 child_num=0 refcnt=20 ilast=0 olast=0 ad=r/2
stat: rxp=1665 txp=2917 rxb=278576 txb=69755
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=7
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0b proto=0 sa=1 ref=4 serial=1 auto-negotiate adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=41599/0B replaywin=1024
    seqno=88b esn=0 replaywin_lastseq=00000680 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42899/43200
  dec: spi=90f03d96 esp=aes key=16 9d7eb233c1d095b30796c3711d53f2fd
    ah=sha1 key=20 d8feacd42b5e0ba8b5e38647b2f2734c94644bd1
  enc: spi=a1bf21c0 esp=aes key=16 d2c0984bf86dc504c5475230b24034f0
    ah=sha1 key=20 3946e4033e1f42b0d9a843b94448f56fd5b57bee
  dec:pkts/bytes=1665/278516, enc:pkts/bytes=4233/264411
  npu_flag=03 npu_rgw=172.16.14.1 npu_lgw=172.16.18.3 npu_selid=1c dec_npuid=1 enc_
npuid=1
-----
name=_OCVPN2-1b ver=2 serial=1b 172.16.18.3:0->172.16.12.1:0 dst_mtu=1500
bound_if=9 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu create_
dev frag-rfc accept_traffic=1 overlay_id=4

proxyid_num=1 child_num=1 refcnt=19 ilast=1 olast=0 ad=r/2
stat: rxp=1 txp=2922 rxb=16430 txb=70173
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=4
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1b proto=0 sa=1 ref=28 serial=1 auto-negotiate adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=41656/0B replaywin=1024
    seqno=890 esn=0 replaywin_lastseq=00000002 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42903/43200
  dec: spi=90f03d9c esp=aes key=16 a655767c1ed6cff4575857eb3981ad81
```

```

ah=sha1 key=20 bfc2bccd7103a201be2641d4c6147d437d2c3f70
enc: spi=a543a7d4 esp=aes key=16 7221b814e483165b01edfdc8260d261a
ah=sha1 key=20 d54819643c2f1b20da2aea4282d50a1f1bc1d72a
dec:pkts/bytes=1/16370, enc:pkts/bytes=4238/265164
npu_flag=03 npu_rgwy=172.16.12.1 npu_lgwy=172.16.18.3 npu_selid=1e dec_npuid=1 enc_
npuid=1

```

### 3. Check the SD-WAN state:

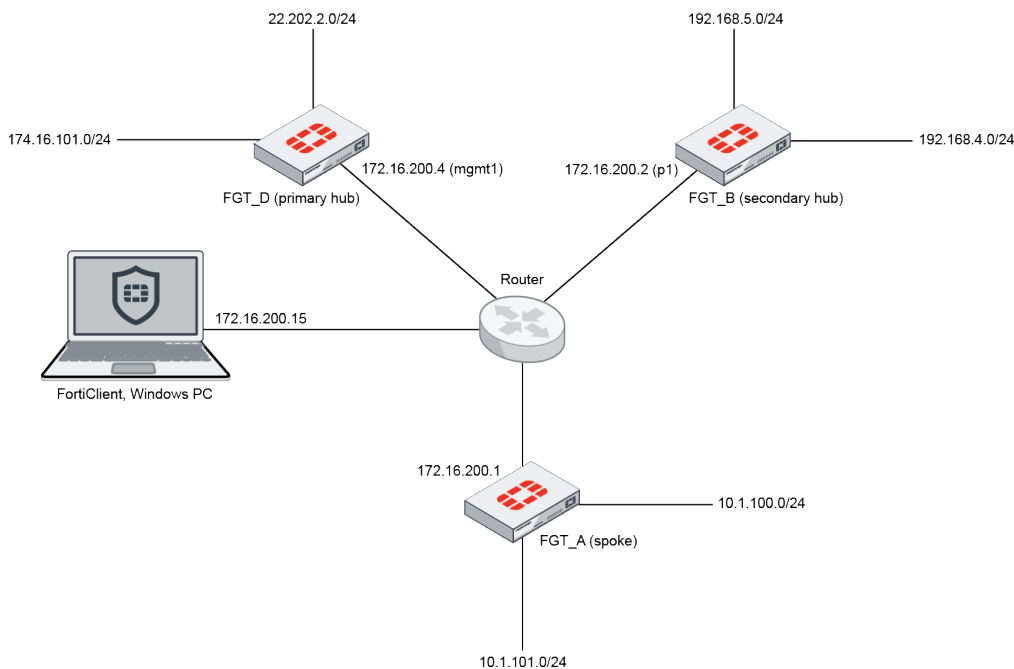
```

FGT_C # diagnose sys virtual-wan-link health-check
Health Check(Default_DNS):
Health Check(Default_Office_365):
Health Check(Default_Gmail):
Health Check(Default_AWS):
Health Check(Default_Google Search):
Health Check(Default_FortiGuard):
Health Check(ocvpn):
Seq(1 _OCVPN2-0a): state(alive), packet-loss(0.000%) latency(0.364), jitter(0.028) sla_
map=0x0
Seq(2 _OCVPN2-0b): state(alive), packet-loss(0.000%) latency(0.287), jitter(0.026) sla_
map=0x0
Seq(3 _OCVPN2-1a): state(dead), packet-loss(100.000%) sla_map=0x0
Seq(4 _OCVPN2-1b): state(dead), packet-loss(100.000%) sla_map=0x0
Seq(4 _OCVPN2-1b_0): state(alive), packet-loss(0.000%) latency(0.289), jitter(0.029)
sla_map=0x0

```

## Allow FortiClient to join OCVPN

Administrators can configure remote access for FortiClient within an OCVPN hub. This provides simple configurations to allow a user group access to an overlay network.



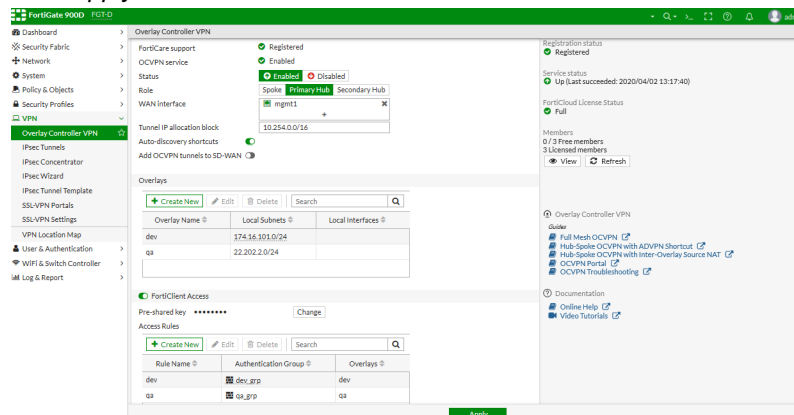
## To configure remote FortiClient access to an OCVPN hub in the GUI:

1. On the primary hub, configure the users and user groups required for the FortiClient dialup user authentication and authorization. In this example, there are two user groups (*dev\_grp* and *qa\_grp*).
2. Go to *VPN > Overlay Controller VPN* and in the *Overlays* section, click *Create New*.
3. Enter a name and the local subnet (174.16.101.0/24 for *dev* and 22.202.2.0/24 for *qa*).
4. Enable *FortiClient Access*.
5. In the *Access Rules* section, click *Create New*.
6. Enter a name, and select the authentication groups and overlays.



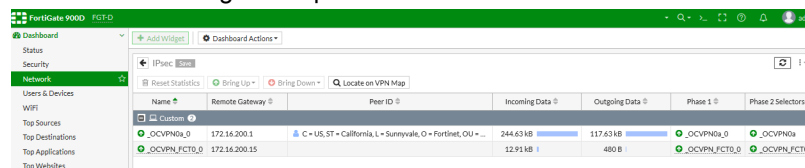
The authentication groups will be used by the IPsec phase 1 interface for authentication, and by firewall policies for authorization. The overlay allows access to the resource.

7. Click *OK*.
8. Create more rules if needed.
9. Click *Apply*.



## To view the tunnel status and activity in the GUI:

1. Go to *Dashboard > Network*.
2. Click the *IPsec* widget to expand to full screen view.



## To configure remote FortiClient access to an OCVPN hub in the CLI:

```
config vpn ocvpn
  set status enable
  set role primary-hub
  set wan-interface "mgmt1"
  set ip-allocation-block 10.254.0.0 255.255.0.0
  config overlays
    edit "dev"
```

```
        config subnets
            edit 1
                set subnet 174.16.101.0 255.255.255.0
            next
        end
    next
    edit "qa"
        config subnets
            edit 1
                set subnet 22.202.2.0 255.255.255.0
            next
        end
    next
end
config forticlient-access
    set status enable
    set psksecret xxxxxxxxxxxxxx
    config auth-groups
        edit "dev"
            set auth-group "dev_grp"
            set overlays "dev"
        next
        edit "qa"
            set auth-group "qa_grp"
            set overlays "qa"
        next
    end
end
end
```

### To view the tunnel status and activity in the CLI:

```
# diagnose vpn ike gateway list
```

```
vd: root/0
name: _OCVPN_FCT0_0
version: 1
interface: mgmt1 4
addr: 172.16.200.4:4500 -> 172.16.200.15:64916
created: 110s ago
xauth-user: usera
groups:
    dev_grp 1
assigned IPv4 address: 10.254.128.1/255.255.255.255
nat: peer
IKE SA: created 1/1  established 1/1  time 20/20/20 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

id/spi: 72 1ccd2abf2d981123/fd8da107f9e4d312
direction: responder
status: established 110-110s ago = 20ms
proposal: aes256-sha256
key: 105a0291b0c05219-3decdf78938a7bea-78943651e1720536-625114d66e46f668
lifetime/rekey: 86400/86019
DPD sent/recv: 00000000/00000af3
```

**To view data on the PC running FortiClient:**

```
C:\ route print
```

```
=====
```

```
IPv4 Route Table
```

```
=====
```

## Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	10.1.100.5	10.1.100.13	281
	<b>10.1.100.0</b>	<b>255.255.255.0</b>	<b>10.254.128.2</b>	<b>10.254.128.1</b>	<b>1</b>
10.1.100.13	255.255.255.255		On-link	10.1.100.13	281
	<b>10.1.101.0</b>	<b>255.255.255.0</b>	<b>10.254.128.2</b>	<b>10.254.128.1</b>	<b>1</b>
10.6.30.0	255.255.255.0		On-link	10.6.30.13	281
10.6.30.13	255.255.255.255		On-link	10.6.30.13	281
10.6.30.255	255.255.255.255		On-link	10.6.30.13	281
10.254.0.0	255.255.0.0		10.254.128.2	10.254.128.1	1
10.254.128.1	255.255.255.255		On-link	10.254.128.1	257
	<b>22.202.2.0</b>	<b>255.255.255.0</b>	<b>10.254.128.2</b>	<b>10.254.128.1</b>	<b>1</b>
127.0.0.0	255.0.0.0		On-link	127.0.0.1	331
127.0.0.1	255.255.255.255		On-link	127.0.0.1	331
127.255.255.255	255.255.255.255		On-link	127.0.0.1	331
172.16.200.4	255.255.255.255		10.1.100.5	10.1.100.13	25
	<b>174.16.101.0</b>	<b>255.255.255.0</b>	<b>10.254.128.2</b>	<b>10.254.128.1</b>	<b>1</b>
224.0.0.0	240.0.0.0		On-link	127.0.0.1	331
224.0.0.0	240.0.0.0		On-link	10.254.128.1	257
224.0.0.0	240.0.0.0		On-link	10.6.30.13	281
224.0.0.0	240.0.0.0		On-link	10.1.100.13	281
255.255.255.255	255.255.255.255		On-link	127.0.0.1	331
255.255.255.255	255.255.255.255		On-link	10.254.128.1	257
255.255.255.255	255.255.255.255		On-link	10.6.30.13	281
255.255.255.255	255.255.255.255		On-link	10.1.100.13	281

## Persistent Routes:

Network	Address	Netmask	Gateway	Address	Metric
	0.0.0.0	0.0.0.0	10.1.100.5	Default	

The PC can access the *dev* resource overlay, but not *qa*:

```
C:\Users\tester>ping 174.16.101.44
```

```
Pinging 174.16.101.44 with 32 bytes of data:
```

```
Reply from 174.16.101.44: bytes=32 time=1ms TTL=63
```

```
Reply from 174.16.101.44: bytes=32 time=1ms TTL=63
```

```
Reply from 174.16.101.44: bytes=32 time=1ms TTL=63
```

```
Reply from 174.16.101.44: bytes=32 time=1ms TTL=63
```

```
Ping statistics for 174.16.101.44:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\Users\tester>ping 22.202.2.2
```

```
Pinging 22.202.2.2 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
Request timed out.
```

```
Ping statistics for 22.202.2.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

## Support SD-WAN interface as a security zone - 6.4.1

SD-WAN is divided into zones. SD-WAN member interfaces are assigned to zones, and zones are used in policies as source and destination interfaces.

You can define multiple zones to group SD-WAN interfaces together, allowing logical groupings for overlay and underlay interfaces. The zones are used in firewall policies to allow for more granular control. SD-WAN members cannot be used directly in policies.

Static routes use the entire SD-WAN, not just individual zones or members.



In the CLI:

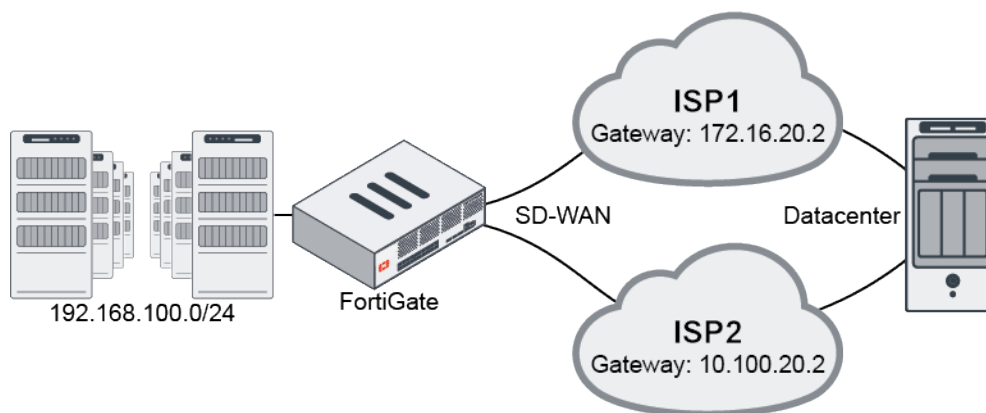
- `config system sdwan` has replaced `config system virtual-wan-link`.
- `diagnose sys sdwan` has replaced `diagnose sys virtual-wan-link`.
- When configuring a static route, the `sdwan` variable has replaced the `virtual-wan-link` variable.

When the Security Fabric is configured, SD-WAN zones are included in the Security Fabric topology views.



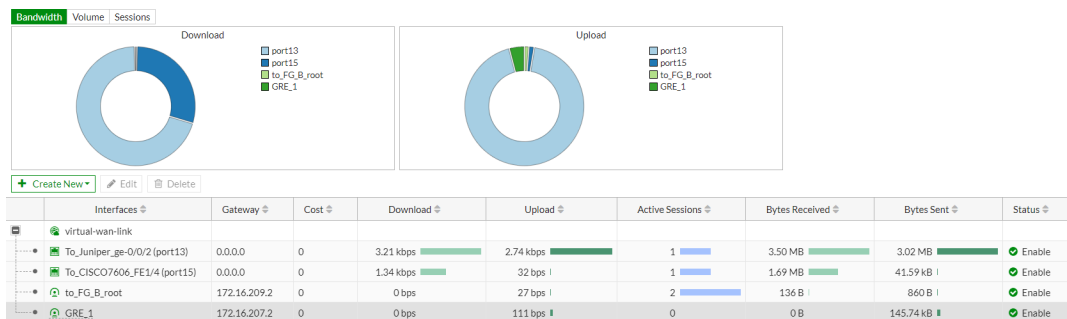
When FortiOS is updated from a previous version:

- SD-WAN interfaces that are not used in a policy are added to the default SD-WAN zone (`virtual-wan-link`).
- SD-WAN interfaces that are used in policies are added to zones that are named after the interface with the prefix `upg-zone-`. For example, SD-WAN interface `GRE_1` will be in zone `upg-zone-GRE_1`. The new zone replaces the SD-WAN interface in the policies.



**To create an SD-WAN zone in the GUI:**

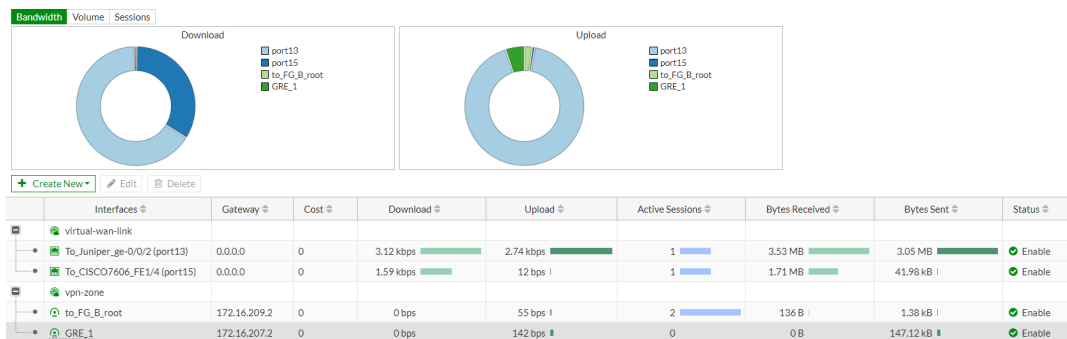
1. Go to *Network > SD-WAN Zones*.  
The default SD-WAN zone is *virtual-wan-link*.



- Click **Create New > SD-WAN Zone**.
- Enter a name for the new zone.
- If SD-WAN members have already been created, add the required members to the zone. Members can also be added to the zone after it has been created by editing the zone, or when creating or editing the member.

The 'New SD-WAN Zone' dialog shows the configuration for a new zone named 'vpn-zone'. The 'Interface members' list includes GRE\_1, to\_FG\_B\_root, and a plus sign for adding more. The 'Select Entries' list on the right shows available interfaces: GRE\_1, To\_Juniper\_ge-0/0/2 (port13), To\_CISCO7606\_FE1/4 (port15), and to\_FG\_B\_root.

- Click **OK**.



## To create an SD-WAN interface member in the GUI:

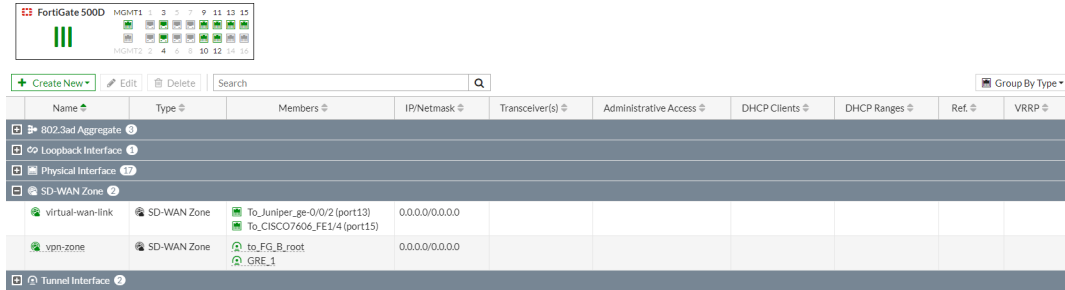
- Go to **Network > SD-WAN Zones**.
- Click **Create New > SD-WAN Member**.
- Select an interface.  
The interface can also be left as *none* and selected later, or click **+VPN** to create an IPsec VPN for the SD-WAN member.
- Select the SD-WAN zone that the member will join. A member can also be moved to a different zone at any time.

The 'New SD-WAN Member' dialog shows the configuration for a new member. The 'Interface' is set to 'vlan100'. The 'SD-WAN Zone' is set to 'virtual-wan-link'. The 'Gateway' is set to 'virtual-wan-link'. The 'Cost' is set to 'vpn-zone'. The 'Status' is set to 'vpn-zone'. The 'SD-WAN Setup Guides' section on the right provides links to various guides.

- Set the **Gateway**, **Cost**, and **Status** as required.

## 6. Click OK.

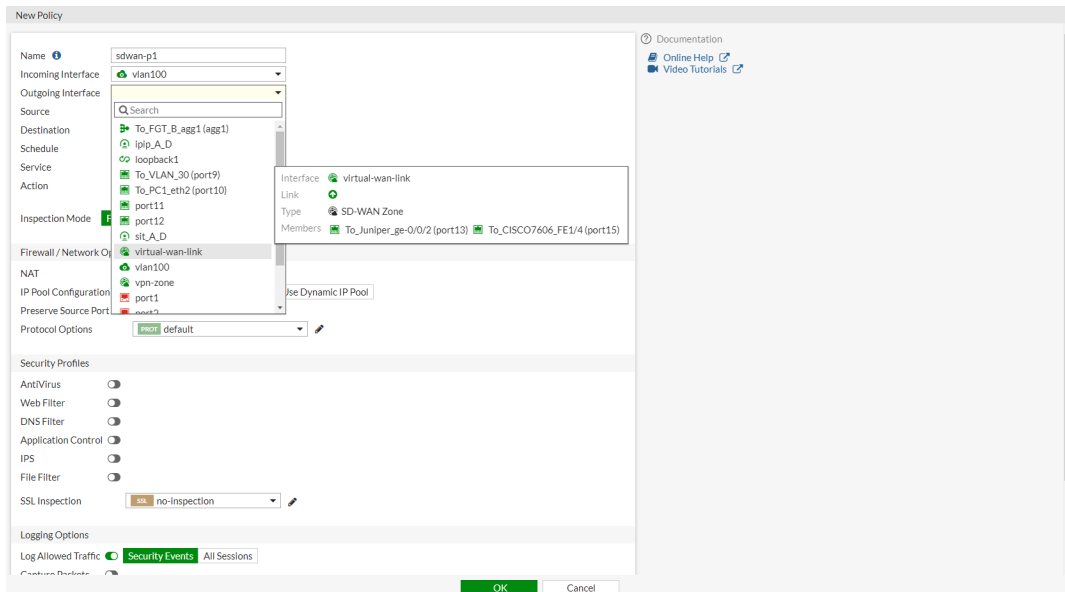
The interface list at *Network > Interfaces* shows the SD-WAN zones and their members.



Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Ref.	VRRP
802.3ad Aggregate									
Loopback Interface									
Physical Interface									
SD-WAN Zone									
virtual-wan-link	SD-WAN Zone	To_Juniper_ge-0/0/2 (port13) To_CISCO7606_FE1/4 (port15)	0.0.0.0/0.0.0.0						
vpn-zone	SD-WAN Zone	to_FG_B_root GRE_1	0.0.0.0/0.0.0.0						
Tunnel Interface									

## To create a policy using the SD-WAN zone in the GUI:

1. Go to *Policy & Objects > Firewall Policy*, *Policy & Objects > Proxy Policy*, or *Policy & Objects > Security Policy*.
2. Click *Create New*.
3. Configure the policy settings as needed, selecting an SD-WAN zone or zones for the incoming and/or outgoing interface.



The 'New Policy' window shows the following configuration:

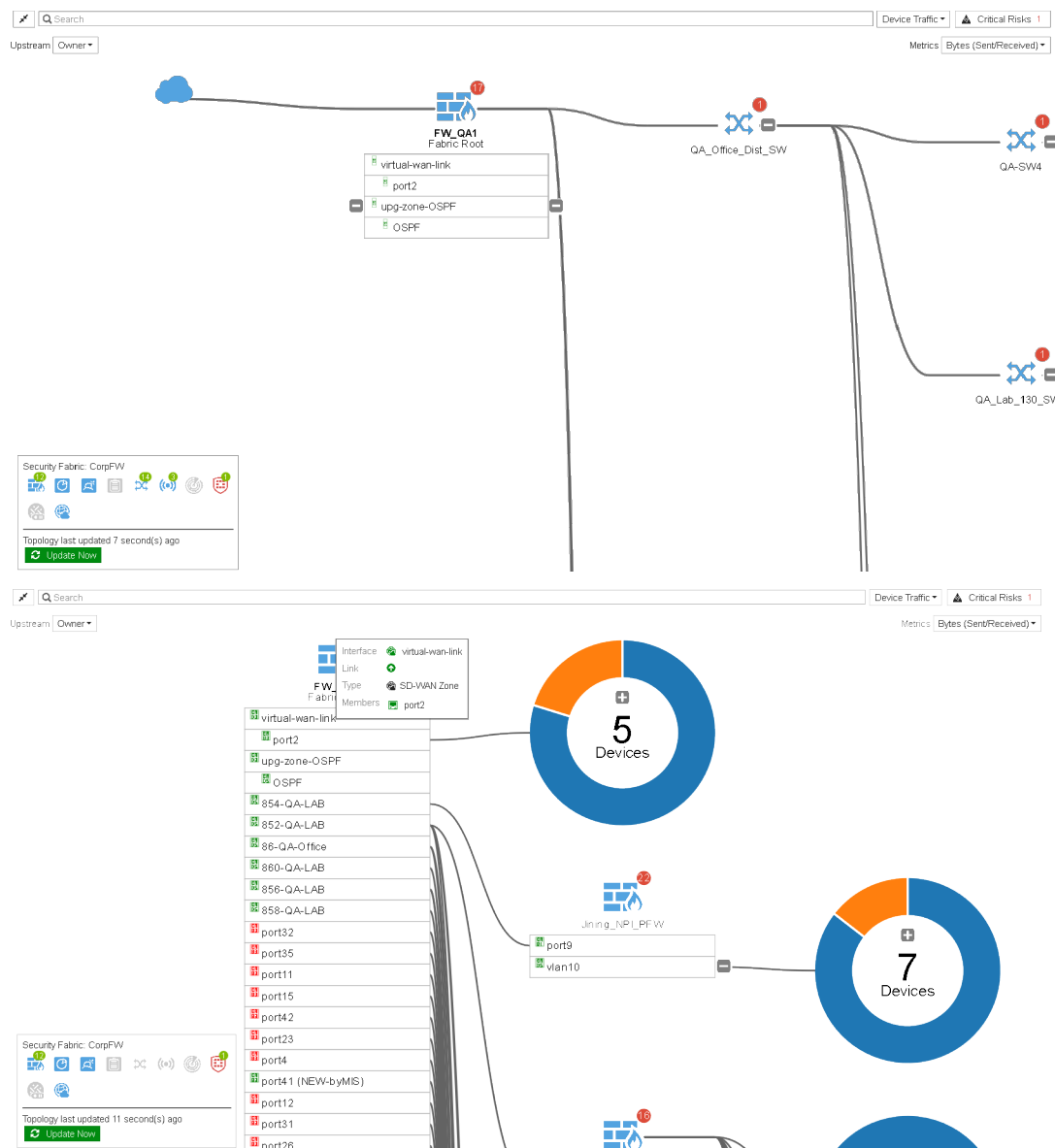
- Name:** sdwan-p1
- Incoming Interface:** vlan100
- Outgoing Interface:** virtual-wan-link
- Source:** To\_FGT\_B\_agg1 (agg1)
- Destination:** To\_VLAN\_30 (port9)
- Schedule:** loopback1
- Service:** port11, port12, st\_A\_D
- Action:** virtual-wan-link
- Inspection Mode:** default
- Firewall / Network Object:** vln100
- NAT:** vln100
- IP Pool Configuration:** port1
- Preserve Source Port:** port1
- Protocol Options:** default
- Security Profiles:**
  - AntiVirus: off
  - Web Filter: off
  - DNS Filter: off
  - Application Control: off
  - IPS: off
  - File Filter: off
  - SSL Inspection: no-inspection
- Logging Options:** Log Allowed Traffic: Security Events, All Sessions

## 4. Click OK.

## To view SD-WAN zones in a Security Fabric topology:

1. Go to *Security Fabric > Physical Topology* or *Security Fabric > Logical Topology*. SD-WAN zones and their members are shown.





## To configure SD-WAN in the CLI:

### 1. Enable SD-WAN and create a zone:

```
config system sdwan
    set status enable
    config zone
        edit "vpn-zone"
        next
    end
end
```

## 2. Configure SD-WAN members and add them to a zone:

```
config system sdwan
  config members
    edit 1
      set interface "to_FG_B_root"
      set zone "vpn-zone"
    next
    edit 2
      set interface "GRE_1"
      set zone "vpn-zone"
    next
  end
end
```

### To create a policy using the SD-WAN zone in the CLI:

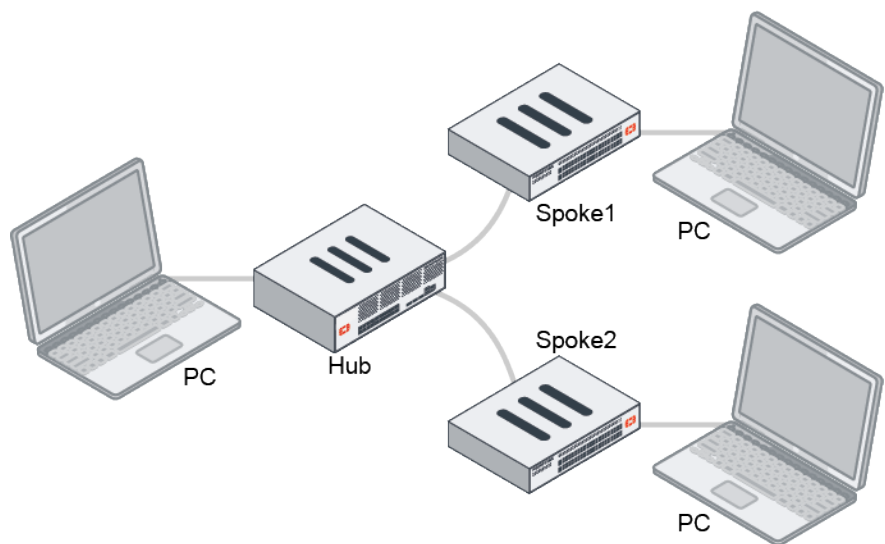
```
config firewall policy
  edit <policy_id>
    set name <policy_name>
    set srcintf internal
    set dstintf vpn-zone
    set srcaddr all
    set dstaddr all
    set action accept
    set schedule always
    set service ALL
    set utm-status enable
    set ssl-ssh-profile <profile_name>
    set av-profile <profile_name>
    set webfilter-profile <profile_name>
    set dnsfilter-profile <profile_name>
    set emailfilter-profile <profile_name>
    set ips_sensor <sensor_name>
    set application-list <app_list>
    set voip-profile <profile_name>
    set logtraffic all
    set nat enable
    set status enable
  next
end
```

## ADVPN hub and spoke VPN Wizard improvements - 6.4.2

When using the IPsec VPN wizard to create a hub and spoke VPN, multiple local interfaces can be selected. At the end of the wizard, changes can be reviewed, real-time updates can be made to the local address group and tunnel interface, and easy configuration keys can be copied for configuring the spokes.

When editing a VPN tunnel, the Hub & Spoke Topology section provides access to the easy configuration keys for the spokes, and allows you to add more spokes.

This example shows the configuration of a hub with two spokes.



**To configure the hub:**

1. Go to *VPN > IPsec Wizard*.
2. Go through the steps of the wizard:
  - a. *VPN Setup*:

<b>Name</b>	hub
<b>Template Type</b>	Hub-and-Spoke
<b>Role</b>	Hub

VPN Creation Wizard

1 VPN Setup

2 Authentication

3 Tunnel Interface

4 Policy & Routing

5 Review Settings

Name

hub

Template type

Site to Site

Hub-and-Spoke

Remote Access

Custom

The Hub-and-Spoke VPN will be set up using auto-discovery with BGP as the routing protocol.

Role

Hub

Spoke

Hub-and-Spoke - FortiGate (Hub)

Hub

This FortiGate

Internet

Spoke1

Remote FortiGate

Spoke2

Remote FortiGate

< Back

Next >

Cancel

- b. *Authentication*:

<b>Incoming Interface</b>	port1
<b>Authentication method</b>	Pre-shared Key
<b>Pre-shared key</b>	<key>

- c. *Tunnel Interface*:

<b>Tunnel IP</b>	10.10.1.1
<b>Remote IP/netmask</b>	10.10.1.2/24

d. *Policy & Routing:*

Multiple local interfaces and subnets can be configured.

<b>Local AS</b>	65400
<b>Local interface</b>	port3 port4
<b>Local subnets</b>	174.16.101.0/24 173.1.1.0/24
<b>Spoke #1 tunnel IP</b>	10.10.1.3
<b>Spoke #2 tunnel IP</b>	10.10.1.4

VPN Creation Wizard

VPN Setup > Authentication > Tunnel Interface > **Policy & Routing** > Review Settings

Local AS: 65400

Local interface: port3, port4

Local subnets: 174.16.101.0/24, 173.1.1.0/24

Spoke #1 tunnel IP: 10.10.1.3

Spoke #2 tunnel IP: 10.10.1.4

Hub-and-Spoke - FortiGate (Hub)

< Back   Next >   Cancel

e. *Review Settings:*

Confirm that the settings look correct, then click *Create*.

3. The summary shows details about the set up hub:

- The *Local address group* and *Tunnel interface* can be edited directly on this page.
- Spoke easy configuration keys can be used to quickly configure the spokes.

VPN Creation Wizard

VPN Setup > Authentication > Tunnel Interface > **Policy & Routing** > Review Settings

✓ The VPN has been set up

**Object Summary**

Phase 1 interface: ✓ hub

Local address group: ✓ hub\_local [Edit]

Phase 2 interface: ✓ hub

Tunnel interface: ✓ hub [Edit]

Remote to local policies: ✓ vpn\_hub\_spoke2hub\_0 (1)  
✓ vpn\_hub\_spoke2hub\_1 (2)

Local to remote policies: ✓ vpn\_hub\_spoke2spoke\_0 (3)

BGP route: ✓ bgp

**Spoke Easy Configuration**

These configuration key(s) are meant for one-time use to automatically configure some of the VPN tunnel settings on your spoke FortiGates.

Spoke #1: eyJodWJHYXRld2F5SXAiOiIxOTIi

Spoke #2: eyJodWJHYXRld2F5SXAiOiIxOTIi

Add Another   Show Tunnel List

4. Click *Show Tunnel List* to go to *VPN > IPsec Tunnels*.

5. Edit the VPN tunnel to add more spokes and to copy the spokes' easy configuration keys.

### To configure the spokes:

1. Go to **VPN > IPsec Wizard**.
2. On the **VPN Setup** page of the wizard, enter the following:

<b>Name</b>	spoke1
<b>Template Type</b>	Hub-and-Spoke
<b>Role</b>	Spoke

3. In the **Easy configuration key** field, paste the **Spoke #1** key from the hub FortiGate, click **Apply**, then click **Next**.

4. Adjust the **Authentication** settings as required, enter the **Pre-shared key**, then click **Next**.
5. Adjust the **Tunnel Interface** settings as required, then click **Next**.
6. Configure the **Policy & Routing** settings, then click **Next**:

<b>Local interface</b>	wan2
<b>Local subnets</b>	10.1.100.0/24

VPN Creation Wizard

VPN Setup Authentication Tunnel Interface **Policy & Routing** Review Settings

Local AS: 65400

Local interface: wan2

Local subnets: 10.1.100.0/24

Hub #1 tunnel IP: 10.10.1.1

Hub-and-Spoke - FortiGate (Spoke)

< Back Next > Cancel

- Review the settings, then click *Create*.
- The summary shows details about the set up spoke. The *Local address group* and *Tunnel interface* can be edited directly on this page.
- Follow the same steps to configure the second spoke.

### To check that the tunnels are created and working:

- On the hub FortiGate, go to *Dashboard > Network* and expand the IPsec widget. The tunnels to the spokes are established.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Hub-and-Spoke - FortiGate (Hub)						
hub_0	172.16.200.1		10.97 kB	5.34 kB	hub_0	hub
hub_1	172.16.200.3		3.51 kB	1.81 kB	hub_1	hub

- On a spoke, go to *Dashboard > Network* and expand the IPsec widget. The tunnel to the hub and the spoke to spoke shortcut are established.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Hub-and-Spoke - FortiGate (Spoke)						
spoke1	172.16.200.4		120 B	5.19 kB	spoke1	spoke1
spoke1_0	172.16.200.3		1.85 MB	1.07 MB	spoke1_0	spoke1

## Allow MAC addresses to be used in SD-WAN rules and policy routes - 6.4.2

Users can select MAC addresses as the source in SD-WAN rules and policy routes.

The FABRIC\_DEVICE address object (a dynamic object that includes the IPs of Security Fabric devices) can be used as a source or destination in SD-WAN rules and policy routes.

The `diagnose ip proute match` command accepts either the IP or MAC address format for the source:

```
diagnose ip proute match <destination> <source> <interface> <protocol> <port>
```

### To configure a MAC address as a source for SD-WAN and a policy route:

- Configure the MAC address:

```
config firewall address
edit "mac-add"
```

```
        set type mac
        set start-mac 70:4c:a5:86:de:56
        set end-mac 70:4c:a5:86:de:56
    next
end
```

## 2. Configure the policy route:

```
config router policy
    edit 3
        set srcaddr "mac-add"
        set gateway 15.1.1.34
        set output-device ha
    next
end
```

## 3. Configure the SD-WAN rule:

```
config system sdwan
    config service
        edit 1
            set dst "all"
            set src "mac-add"
            set priority-members 1
        next
        edit 2
            set dst "FABRIC_DEVICE"
            set priority-members 2
        next
    end
end
```

### To verify the policy route matching for a MAC address:

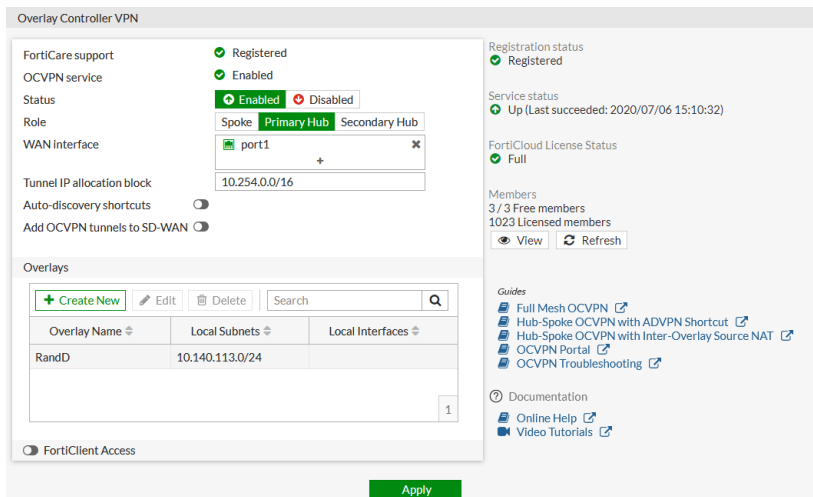
```
# diagnose ip proute match 3.1.1.34 70:4c:a5:86:de:56 port3 22 6
dst=3.1.1.34 src=0.0.0.0 smac=70:4c:a5:86:de:56 iif=11 protocol=22 dport=6
id=00000003 type=Policy Route
seq-num=3
```

## Up to 1024 spokes in OCVPN - 6.4.2

The FortiCloud Premium license increases the spoke limit from 512 to 1024, allowing you to deploy two hubs and 1024 spokes.

On the FortiCloud OCVPN-Portal, select an overlay to view a list of all of the hubs and spokes.

On the FortiGate, go to *VPN > Overlay Controller VPN* to see the license status and the total number of members.



## SD-WAN enhancements - 6.4.2

SD-WAN has been enhanced to include more load balancing hash methods, more health check protocols, and an option to set the minimum number of links required for a rule to take effect.

- [Minimum number of links for a rule to take effect on page 178](#)
- [Load balance hash methods on page 179](#)
- [Health check options on page 180](#)

### Minimum number of links for a rule to take effect

You can specify the number of links that must be up for an SD-WAN to take effect.

For example: Ports 1 to 4 each have 10Mbps of bandwidth, and port 5 has 50Mbps. An application requires 35Mbps of bandwidth, so the SD-WAN rule balances the traffic between ports 1 to 4. If one of the links goes down, all of the traffic must be passed to port 5.

#### To set the minimum number of links in a rule:

```
config system sdwan
    config service
        edit 1
            set mode load-balance
            set minimum-sla-meet-members 4
            set dst <destination>
            config sla
                edit <sla>
                    set id <id>
                next
            end
            set priority-members 1 2 3 4
        next
    end
end
```



## Load balance hash methods

The load balancing strategy in SD-WAN rules can be configured to balance based on the best bandwidth, source IP address, or source and destination IP addresses hash methods.

Hash methods include:

round-robin	All traffic are distributed to selected interfaces in equal portions and circular order.
source-ip-based	All traffic from a source IP is sent to the same interface.
source-dest-ip-based	All traffic from a source IP to a destination IP is sent to the same interface.
inbandwidth	All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.
outbandwidth	All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.
bibandwidth	All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.

### To use the load balancing algorithm to steer traffic to an IPv4 address based on a hash method:

```
config system sdwan
  config service
    edit 1
      set addr-mode ipv4
      set mode load-balance
      set hash-mode {round-robin | source-ip-based | source-dest-ip-based |
inbandwidth | outbandwidth | bibandwidth}
      set protocol 1
      set dst "80.1.1.0/24"
      set src "70.1.1.0/24"
      config sla
        edit "h1"
          set id 1
        next
      end
      set priority-members 1 2 3 4
    next
  end
end
```

### To use the load balancing algorithm to steer traffic to an IPv6 address based on various hash methods:

```
config system sdwan
  config service
    edit 11
      set addr-mode ipv6
      set mode load-balance
      set hash-mode {round-robin | source-ip-based | source-dest-ip-based |
inbandwidth | outbandwidth | bibandwidth}
      config sla
        edit "h6_dns1"
          set id 1
```

```

        next
    end
    set priority-members 1 2
    set dst6 "2032::11"
next
end
end

```

## Health check options

Health checks include several protocols and protocol specific options.

The health check protocol options include:

ping	Use PING to test the link with the server.
tcp-echo	Use TCP echo to test the link with the server.
udp-echo	Use UDP echo to test the link with the server.
http	Use HTTP-GET to test the link with the server.
twamp	Use TWAMP to test the link with the server.
dns	Use DNS query to test the link with the server. The FortiGate sends a DNS query for an A Record and the response matches the expected IP address.
tcp-connect	Use a full TCP connection to test the link with the server. The method to measure the quality of the TCP connection can be: <ul style="list-style-type: none"> <li><code>half-open</code>: FortiGate sends SYN and gets SYN-ACK. The latency is based on the round trip between SYN and SYN-ACK (default).</li> <li><code>half-close</code>: FortiGate sends FIN and gets FIN-ACK. The latency is based on the round trip between FIN and FIN-ACK.</li> </ul>
ftp	Use FTP to test the link with the server. The FTP mode can be: <ul style="list-style-type: none"> <li><code>passive</code>: The FTP health-check initiates and establishes the data connection (default).</li> <li><code>port</code>: The FTP server initiates and establishes the data connection.</li> </ul>

### To use UDP-echo and TCP-echo as health checks:

```

config system sdwan
    set status enable
    config health-check
        edit "h4_udp1"
            set protocol udp-echo
            set port 7
            set server <server>
        next
        edit "h4_tcp1"
            set protocol tcp-echo
            set port 7
            set server <server>
    end
end

```

```
        next
        edit "h6_udp1"
            set addr-mode ipv6
            set server "2032::12"
            set protocol udp-echo
            set port 7
        next
    end
end
```

**To use DNS as a health check, and define the IP address that the response must match:**

```
config system sdwan
    set status enable
    config health-check
        edit "h4_dns1"
            set protocol dns
            set dns-request-domain "ip41.forti2.com"
            set dns-match-ip 1.1.1.1
        next
        edit "h6_dns1"
            set addr-mode ipv6
            set server "2000::15.1.1.4"
            set protocol dns
            set port 53
            set dns-request-domain "ip61.xxx.com"
        next
    end
end
```

**To use TCP Open (SYN/SYN-ACK) and TCP Close (FIN/FIN-ACK) to verify connections:**

```
config system sdwan
    set status enable
    config health-check
        edit "h4_tcpconnect1"
            set protocol tcp-connect
            set port 443
            set quality-measured-method {half-open | half-close}
            set server <server>
        next
        edit "h6_tcpconnect1"
            set addr-mode ipv6
            set server "2032::13"
            set protocol tcp-connect
            set port 444
            set quality-measured-method {half-open | half-close}
        next
    end
end
```

**To use active or passive mode FTP to verify connections:**

```
config system sdwan
    set status enable
    config health-check
```

```

edit "h4_ftp1"
    set protocol ftp
    set port 21
    set user "root"
    set password *****
    set ftp-mode {passive | port}
    set ftp-file "1.txt"
    set server <server>
next
edit "h6_ftp1"
    set addr-mode ipv6
    set server "2032::11"
    set protocol ftp
    set port 21
    set user "root"
    set password *****
    set ftp-mode {passive | port}
    set ftp-file "2.txt"
next
end
end

```

## Define SD-WAN duplication rules to duplicate packets on other members of the SD-WAN zone - 6.4.2

When duplication rules are used, packets are duplicated on other good links within the SD-WAN zone and de-duplicated on the destination FortiGate. Use `force` mode to force duplication on other links within the SD-WAN zone, or use `on-demand` mode to trigger duplication only when SLA fails on the selected member.

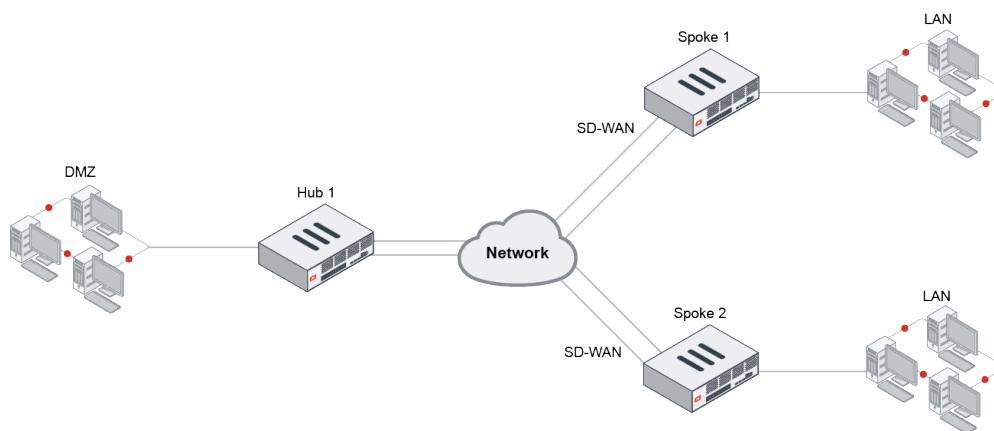
The duplication rule is configured in the CLI by using the `config duplication` parameter within `config system sdwan`. The following parameters can be configured for `config duplication`:

Parameter	Description
<code>srcaddr</code>	Source address or address group names.
<code>dstaddr</code>	Destination address or address group names.
<code>srcaddr6</code>	Source address6 or address6 group names.
<code>dstaddr6</code>	Destination address6 or address6 group names.
<code>srcintf</code>	Incoming (ingress) interfaces or zones.
<code>dstintf</code>	Outgoing (egress) interfaces or zones.
<code>service</code>	Service and service group names.
<code>packet-duplication</code>	Configure packet duplication method. <ul style="list-style-type: none"> <li><code>disable</code>: Disable packet duplication.</li> <li><code>force</code>: Duplicate packets across all interface members of the SD-WAN zone.</li> <li><code>on-demand</code>: Duplicate packets across all interface members of the SD-WAN zone based on the link quality.</li> </ul>
<code>packet-de-duplication</code>	Enable/disable discarding of packets that have been duplicated.

The `duplication-max-num <integer>` parameter within `config system sdwan` is the maximum number of interface members a packet is duplicated in the SD-WAN zone (2 - 4, default = 2). If this value is set to 3, the original packet plus two more copies are created. If there are three member interfaces in the SD-WAN zone and the `duplication-max-num` is set to 2, the packet duplication follows the configuration order, so the packets are duplicated on the second member.

## Example

The packet duplication feature works best in a spoke-spoke or hub-spoke topology. In this example, a hub and spoke ADVPN topology is used. Before shortcuts are established, the Hub forwards the duplicate packets from Spoke 1 to Spoke 2. Once shortcuts are established, the Hub is transparent. Duplicate packets are exchanged directly between the spokes.



### To use packet duplication between Spoke 1 and Spoke 2:

#### 1. Configure Spoke 1:

```
config system sdwan
  set status enable
  config zone
    edit "virtual-wan-link"
    next
    edit "sdwanzone_v4"
    next
  end
  config members
    edit 1
      set interface "t1"
      set zone "sdwanzone_v4"
    next
    edit 4
      set interface "t21"
      set zone "sdwanzone_v4"
    next
    edit 2
      set interface "t2"
      set zone "sdwanzone_v4"
    next
  end
```

```

config health-check
    edit "h1"
        set server "10.34.1.1"
        set interval 1000
        set failtime 10
        set members 1 2
        config sla
            edit 1
                set packetloss-threshold 40
            next
        end
    next
end
config duplication
    edit 1
        set srcaddr "all"
        set dstaddr "all"
        set srcintf "port1"
        set dstintf "sdwanzone_v4"
        set service "ALL"
        set packet-duplication force
        set packet-de-duplication enable
    next
end
end

```

2. Configure Spoke 2 with similar settings.

## Allow packet duplication on SD-WAN based on SD-WAN rules - 6.4.3

SD-WAN duplication rules can specify SD-WAN service rules to trigger packet duplication. This allows the duplication to occur based on an SD-WAN rule instead of the source, destination, and service parameters in the duplication rule.

1. Packets can be forced to duplicate to all members of the same SD-WAN zone. See [Duplicate packets on other zone members](#) for details.

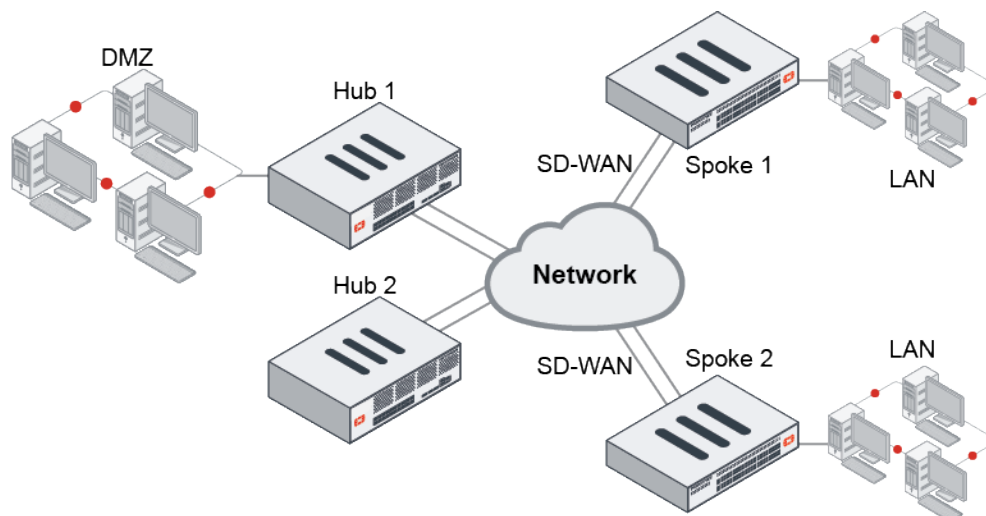
For example, in Spoke 1 set `packet-duplication` to `force` so that when a client sends a packet to the server, it is duplicated to all members of the same zone as long as its health check is alive. If a member's health check is dead, then the member is removed from the SD-WAN duplication zone.

2. Packets can be duplicated to other members of the SD-WAN zone only when the condition of the link is not good enough.

Set `packet-duplication` to `on-demand` so that, when the SLA of the member does not match (`sla_map=0`) the packet is duplicated, but when the SLA does match (`sla_map!=0`) the packet is not duplicated.

3. Packets can be duplicated to all members of the same SD-WAN zone when the traffic matches one or more regular SD-WAN service rules.

The following example shows the third type of packet duplication.



In this example, SD-WAN is configured with three members: vpn1, vpn2, and vpn3. Service rule 1 controls all traffic from 10.100.20.0/24 to 172.16.100.0/24 using member 1.

To send a duplicate of the traffic that matches service rule 1 using member 2, members 1 and 2 are added to the same SD-WAN zone, and a duplicate rule is configured with service-id set to 1.

#### To send a duplicate of the traffic that matches service rule 1 using member 2:

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "zone2"
        next
    end
    config members
        edit 1
            set interface "vpn1"
        next
        edit 2
            set interface "vpn2"
        next
        edit 3
            set interface "vpn3"
            set zone "zone2"
        next
    end
    config service
        edit 1
            set dst "172.16.100.0"
            set src "10.100.20.0"
            set priority-members 1
        next
    end
    config duplication
        edit 1
            set service-id 1
```

```

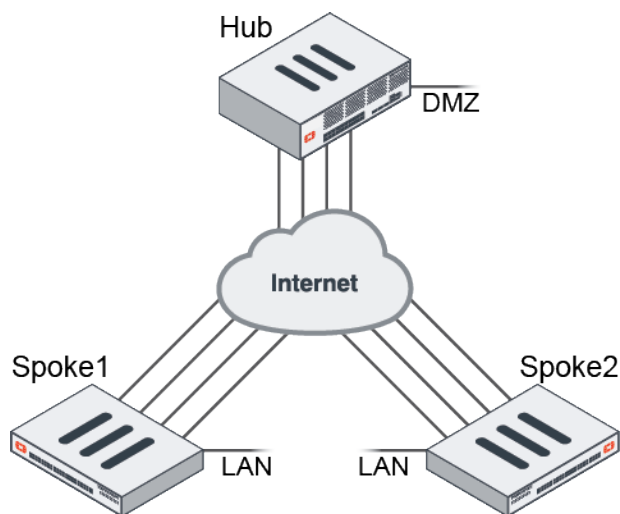
        set packet-duplication force
    next
end
end

```

## BGP additional path limit increased to 255 - 6.4.3

Up to 255 BGP paths can be selected and advertised. Previously, the limit was eight paths.

In this example topology, each spoke has multiple VPN tunnels that connect to the hub with ADVPN and runs spoke-hub to establish multiple BGP neighbors on all of the tunnels.



### To set the additional path limit to 255:

```

config router bgp
    set additional-path-select 255
    config {neighbor | neighbor-group}
        edit <ip address>
            set adv-additional-path 255
        next
    end
end
end

```

## SD-WAN IPv6 route tag - 6.4.4

The `route-tag` is a mechanism to map a BGP community string to a specific tag. The string may correspond to a specific network that a BGP router advertised. With this tag, an SD-WAN service rule can be used to define specific traffic handling to that network. IPv6 route tags are now supported. The SD-WAN link quality information is also shown in IPv6 traffic logs.



## To configure an IPv6 route tag:

### 1. Configure the route map:

```
config router route-map
  edit "comm1"
    config rule
      edit 1
        set match-community "30:5"
        unset set-ip-nexthop
        unset set-ip6-nexthop
        unset set-ip6-nexthop-local
        unset set-originator-id
        set set-route-tag 15
      next
      edit 2
        unset set-ip-nexthop
        unset set-ip6-nexthop
        unset set-ip6-nexthop-local
        unset set-originator-id
      next
    end
  next
end
```

### 2. Configure SD-WAN:

```
config system sdwan
  set status enable
  config zone
    edit "virtual-wan-link"
      next
    end
  config members
    edit 1
      set interface "R150"
      set gateway 10.100.1.1
      set gateway6 2004:10:100:1::1
    next
    edit 2
      set interface "R160"
      set gateway 10.100.1.5
      set gateway6 2004:10:100:1::5
      set priority 20
    next
  end
  config health-check
    edit "ping6"
      set addr-mode ipv6
      set server "2000:10:100:2::22"
      set members 1 2
    next
  end
  config service
    edit 1
      set addr-mode ipv6
      set route-tag 15
```

```

        set priority-members 1 2
    next
end
end

```

### 3. Verify the traffic log:

```

1: date=2020-11-18 time=17:30:39 eventtime=1605749439420496570 tz="-0800"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=2000:172:16:205::11 identifier=523 srcintf="port10" srcintfrole="undefined"
dstip=2008:3:3:3::3 dstintf="R150" dstintfrole="undefined" sessionid=3781 proto=58
action="accept" policyid=1 policytype="policy" poluuid="0fda65ea-4077-51e9-006b-
da60dff24c0d" service="PING6" dstcountry="Reserved" srccountry="Reserved"
trandisp="noop" duration=8 sentbyte=104 rcvdbyte=104 sentpkt=1 rcvdpkt=1 vwliid=22
vwlquality="Seq_num(1 R150), alive, sla(0x1), gid(0), cfg_order(0), cost(0), selected"
appcat="unscanned"

```

## REST API to monitor SD-WAN SLAs for ADVPN shortcuts - 6.4.5

The SD-WAN REST API for `health-check` and `sla-log` now exposes ADVPN shortcut information in its result. The `child_intf` attribute returns the statistics for the corresponding shortcuts. The following command displays real-time SLA information for ADVPN shortcuts:

```
# diagnose sys sdwan sla-log <health check name> <sequence number> <child name>
```

### api/v2/monitor/virtual-wan/health-check

```

{
  "http_method": "GET",
  "results": {
    "ping": {
      "spoke11-pl": {
        "status": "up",
        "latency": 0.13406667113304138,
        "jitter": 0.023000005632638931,
        "packet_loss": 0,
        "packet_sent": 29722,
        "packet_received": 29718,
        "sla_targets_met": [
          1
        ],
        "session": 2,
        "tx_bandwidth": 1353,
        "rx_bandwidth": 1536,
        "state_changed": 1614798274,
        "child_intf": {
          "spoke11-pl_0": {
            "status": "up",
            "latency": 0.12929999828338623,
            "jitter": 0.028200000524520874,
            "packet_loss": 0,
            "packet_sent": 29626,
            "packet_received": 29625,
            "sla_targets_met": [
              1
            ]
          }
        }
      }
    }
  }
}

```

```

        ],
        "session":0,
        "tx_bandwidth":2608,
        "rx_bandwidth":1491,
        "state_changed":0
    }
}
},
"spoke12-p1":{
    "status":"up",
    "latency":0.11356667429208755,
    "jitter":0.015699999406933784,
    "packet_loss":0,
    "packet_sent":29722,
    "packet_received":29717,
    "sla_targets_met":[
        1
    ],
    "session":2,
    "tx_bandwidth":1353,
    "rx_bandwidth":1536,
    "state_changed":1614798274,
    "child_intf":{
        "spoke12-p1_0":{
            "status":"up",
            "latency":0.095466658473014832,
            "jitter":0.0092999991029500961,
            "packet_loss":0,
            "packet_sent":29687,
            "packet_received":29686,
            "sla_targets_met":[
                1
            ],
            "session":0,
            "tx_bandwidth":1309,
            "rx_bandwidth":2553,
            "state_changed":0
        }
    }
}
},
"vdom":"root",
"path":"virtual-wan",
"name":"health-check",
"status":"success",
"serial":"FG100FTK19000000",
"version":"v6.4.5",
"build":1822

```

### FortiOS CLI output:

```

# diagnose sys sdwan health-check
Health Check(ping):
Seq(1 spoke11-p1): state(alive), packet-loss(0.000%) latency(0.156), jitter(0.043) sla_
map=0x1

```

```
Seq(1 spoke11-p1_0): state(alive), packet-loss(0.000%) latency(0.128), jitter(0.024) sla_
map=0x1
Seq(2 spoke12-p1): state(alive), packet-loss(0.000%) latency(0.125), jitter(0.028) sla_
map=0x1
Seq(2 spoke12-p1_0): state(alive), packet-loss(0.000%) latency(0.093), jitter(0.008) sla_
map=0x1
```

### api/v2/monitor/virtual-wan/sla-log

```
{
  "http_method": "GET",
  "results": [
    {
      "name": "ping",
      "interface": "spoke11-p1",
      "logs": [
        {
          "timestamp": 1614813142,
          "link": "up",
          "latency": 0.13763333857059479,
          "jitter": 0.02996666356921196,
          "packetloss": 0
        }
      ],
      "child_intf": {
        "spoke11-p1_0": [
          {
            "timestamp": 1614813142,
            "link": "up",
            "latency": 0.12413334846496582,
            "jitter": 0.028366668149828911,
            "packetloss": 0
          }
        ]
      }
    },
    {
      "name": "ping",
      "interface": "spoke12-p1",
      "logs": [
        {
          "timestamp": 1614813143,
          "link": "up",
          "latency": 0.11373332887887955,
          "jitter": 0.023099998012185097,
          "packetloss": 0
        }
      ],
      "child_intf": {
        "spoke12-p1_0": [
          {
            "timestamp": 1614813143,
            "link": "up",
            "latency": 0.0930333212018013,
            "jitter": 0.011033335700631142,
            "packetloss": 0
          }
        ]
      }
    }
  ],
  "vdom": "root",
```

```
"path":"virtual-wan",
"name":"sla-log",
"status":"success",
"serial":"FG100FTK19000000",
"version":"v6.4.5",
"build":1822
```

**FortiOS CLI output:**

```
# diagnose sys sdwan sla-log ping 1 spoke11-p1_0
Timestamp: Wed Mar  3 15:35:20 2021, vdom root, health-check ping, interface: spoke11-p1_0,
status: up, latency: 0.135, jitter: 0.029, packet loss: 0.000%.

# diagnose sys sdwan sla-log ping 2 spoke12-p1_0
Timestamp: Wed Mar  3 15:36:08 2021, vdom root, health-check ping, interface: spoke12-p1_0,
status: up, latency: 0.095, jitter: 0.010, packet loss: 0.000%.
```

## General

This section includes information about general network related new features:

- [Route leaking between VRFs on page 191](#)
- [IBGP and EBGP support in VRF on page 193](#)
- [Set minimum RIP update timer to one second on page 196](#)
- [DHCP client options on page 196](#)
- [Assign a subnet to FortiGate with the FortiIPAM service 6.4.1 on page 197](#)
- [VRF GUI support 6.4.2 on page 204](#)
- [Determine if recursive distance is evaluated in BGP's next hops under ECMP 6.4.2 on page 206](#)
- [PRP on SoC4 models 6.4.3 on page 207](#)
- [FN-TRAN-DSL module on FG-80F and FGR-60F-3G4G 6.4.9 on page 208](#)
- [Reset the VLAN DEI bit when passing through a FortiGate in NAT mode 6.4.9 on page 210](#)
- [FS-TRANS-FX module on FGR-60F and FGR-60F-3G4G 6.4.9 on page 211](#)
- [Inspect double-tagged traffic on virtual wire pairs 6.4.9 on page 212](#)
- [Support 802.1X on virtual switch for certain NP6 platforms 6.4.10 on page 213](#)

## Route leaking between VRFs

This feature provides generic route leaking capabilities between locally defined VRFs (VRF-lite). If VRF leaking is not configured, VRFs are isolated.

In this example, interface *npu0\_vlink0* belongs to VRF 10 and is used to leak 1.2.2.2/32 from VRF10 to VRF20, and interface *npu0\_vlink1* belongs to VRF 20 and is used to leak 172.28.1.0/24 from VRF20 to VRF10. So, VRF10 can see 172.28.1.0/24, and VRF20 can see 1.2.2.2/32.

**To configure VRF leaking:****1. Configure the prefix list and route map to filter what will be leaked:**

```
config router prefix-list
  edit "1"
    config rule
      edit 1
        set prefix 1.2.2.2 255.255.255.255
      next
    end
  next
  edit "2"
    config rule
      edit 1
        set prefix 172.28.1.0 255.255.255.0
      next
    end
  next
end

config router route-map
  edit "from10"
    config rule
      edit 1
        set match-ip-address "1"
      next
    end
  next
  edit "from20"
    config rule
      edit 1
        set match-ip-address "2"
      next
    end
  next
end
```

**2. Configure the VDOM link interfaces for the leaking and routing:**

```
config system interface
  edit "np0_vlink0"
    set vdom "root"
    set vrf 10
    set ip 172.16.201.1 255.255.255.0
    set allowaccess ping https ssh snmp http
  next
  edit "np0_vlink1"
    set vdom "root"
    set vrf 20
    set ip 172.16.201.2 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
  next
end
```

### 3. Configure the BGP VRF leak:

```

config router bgp
    set as 44
    set router-id 4.4.4.4
    config neighbor
        edit "172.16.200.1"
            set soft-reconfiguration enable
            set remote-as 11
            set update-source "port1"
        next
        edit "172.16.202.1"
            set soft-reconfiguration enable
            set remote-as 22
            set update-source "port3"
        next
    end
    config vrf-leak
        edit "10"
            config target
                edit "20"
                    set route-map "from10"
                    set interface "npu0_vlink0"
                next
            end
        next
        edit "20"
            config target
                edit "10"
                    set route-map "from20"
                    set interface "npu0_vlink1"
                next
            end
        next
    end
end
end

```

**4. Confirm that the filtered routed leaked as expected:**

```
# get router info routing-table all
Routing table for VRF=10
B      1.1.1.1/32 [20/0] via 172.16.200.1, port1, 01:03:16
B      1.2.2.2/32 [20/0] via 172.16.200.1, port1, 01:03:16
B      172.28.1.0/24 [20/0] via 172.16.201.2, npu0_vlink0, 00:00:17
<<<<<<<<<<<Leaked into VRF10 from VRF20

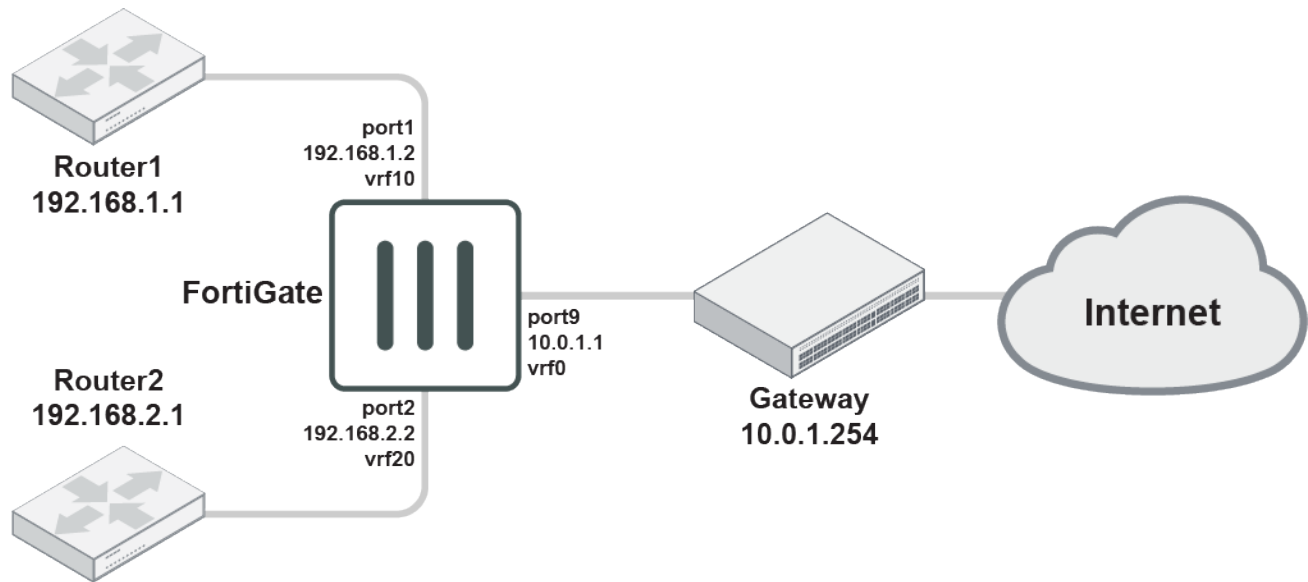
Routing table for VRF=20
B      1.2.2.2/32 [20/0] via 172.16.201.1, npu0_vlink1, 00:00:15   <<<<<<<<<<<Leaked
into VRF 20 from VRF10
B      172.28.1.0/24 [20/0] via 172.16.202.1, port3, 01:03:16
B      172.28.2.0/24 [20/0] via 172.16.202.1, port3, 01:03:16
```

## IBGP and EBGP support in VRF

Support is included for internal and external border gateway protocols (IBGP and EBGP) in virtual routing and forwarding (VRF).

FortiGate can establish neighbor connections with other FortiGates or routers, and the learned routes are put into different VRF tables according to the neighbor's settings.

This example uses the following topology:



- BGP routes learned from the Router1 neighbor are put into vrf10.
- BGP routes learned from the Router2 neighbor are put into vrf20.

#### To configure this example:

```

config system interface
    edit port1
        set vrf 10
    next
    edit port2
        set vrf 20
    next
end

config router bgp
    config neighbor
        edit "192.168.1.1"
            set update-source port1
        next
        edit "192.168.2.1"
            set interface port2
        next
    end
end

```

#### Results

Using the above topology:

- Both Router1 and Router2 establish OSPF and BGP neighbor with the FortiGate.
- Router1 advertises 10.10.1.0/24 into OSPF and 10.10.2.0/24 into BGP.



- Router2 advertises 20.20.1.0/24 into OSPF and 20.20.2.0/24 into BGP.

When port1 and port2 have not set VRF, all of the routing is in VRF=0:

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*    0.0.0.0/0 [5/0] via 10.0.1.254, port9
C     10.0.1.0/24 is directly connected, port9
O     10.10.1.0/24 [110/10] via 192.168.1.1, port1, 00:18:31
B     10.10.2.0/24 [20/200] via 192.168.1.1, port1, 00:01:31
O     20.20.1.0/22 [110/10] via 192.168.2.1, port2, 00:19:05
B     20.20.2.0/24 [20/200] via 192.168.2.1, port2, 00:01:31
C     192.168.1.0/24 is directly connected, port1
C     192.168.2.0/24 is directly connected, port2
```

After VRF is set for BGP, BGP routes are added to the VRF tables along with OSPF and connected routes:

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*    0.0.0.0/0 [5/0] via 10.0.1.254, port9
C     10.0.1.0/24 is directly connected, port9

Routing table for VRF=10
O     10.10.1.0/24 [110/10] via 192.168.1.1, port1, 00:18:31
B     10.10.2.0/24 [20/200] via 192.168.1.1, port1, 00:01:31
C     192.168.1.0/24 is directly connected, port1

Routing table for VRF=20
O     20.20.1.0/22 [110/10] via 192.168.2.1, port2, 00:19:05
B     20.20.2.0/24 [20/200] via 192.168.2.1, port2, 00:01:31
C     192.168.2.0/24 is directly connected, port2
```

## BGP neighbor groups

This feature is also supported in the BGP neighbor groups. For example:

```
config router bgp
  config neighbor-group
    edit "FGT"
      set update-source "port1"
    next
  end
  config neighbor-range
    edit 1
```

```

        set prefix 172.16.201.0 255.255.255.0
        set neighbor-group "FGT"
    next
end
end

```

Note that the `set interface` command is not supported.

## Set minimum RIP update timer to one second

The RIP update timer can be set to a minimum value of 1 second. The previous minimum timer value was 5 seconds.

**To set the RIP timer value to one second:**

```

config router rip
    set update-timer 1
end

```

## DHCP client options

When an interface is in DHCP addressing mode, DHCP client options can be configured in the CLI. For example, a vendor class identifier (usually DHCP client option 60) can be specified so that a request can be matched by a specific DHCP offer.

Multiple options can be configured, but any options not recognized by the DHCP server are discarded.

**To configure client option 60 - vendor class identifier:**

```

config system interface
    edit port1
        set vdom vdom1
        set mode dhcp
        config client-options
            edit 1
                set code 60
                set type hex
                set value aabbccdd
            next
        end
        set type physical
        set snmp-index 4
    next
end

```

Variable	Description
code <integer>	DHCP client option code (0 - 255, default = 0). See <a href="#">Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters</a> for a list of possible options.
type {hex   string   ip   fqdn}	DHCP client option type (default = hex).

Variable	Description
value <string>	DHCP client option value.
ip <ip>	DHCP client option IP address. This option is only available when <code>type</code> is <code>ip</code> .

## Assign a subnet to FortiGate with the FortiPAM service - 6.4.1

The FortiPAM (IP Address Management) service automatically assigns subnets to FortiGate to prevent duplicate IP addresses from overlapping within the same Security Fabric.

After the FortiPAM registration is synced to FortiGuard from FortiCare, FortiGate can use FortiPAM to automatically assign IP addresses based on the configured network size for the FortiGate interface.

### Requirements:

Register the FortiPAM service for FortiGate in FortiCare.



FortiPAM is a paid service.

### To verify the FortiPAM service registration in the GUI:

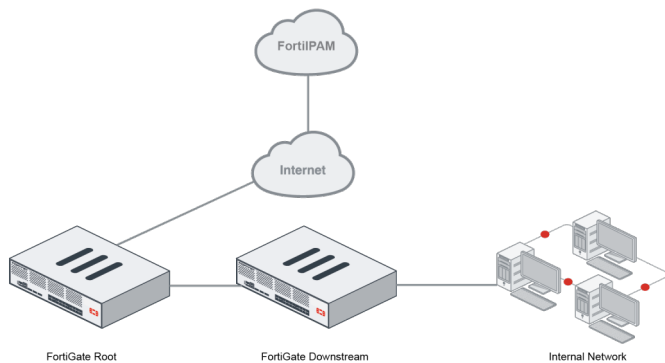
1. Go to *System > FortiGuard* to verify the FortiPAM service is registered. If the service is registered, the *FortiPAM* area at the bottom of the page displays a check mark as well as the license expiry date.

The screenshot shows the FortiGuard Distribution Network interface. On the left, a list of services is shown with their status and license expiry dates. On the right, a table displays the traffic volume for each service over the last 24 hours.

Service	Traffic Volume (Last 24 hours)
FortiCare	0 B
FortiCloud Log	27.75 kB
FortiGuard.com	1.54 MB
FortiGuard Download	18.50 MB
FortiGuard Query	11.64 kB
FortiSandbox Cloud	0 B
OCVPN	0 B
SDNS	0 B
FortiToken Registration	0 B
SMS Service	0 B

At the bottom of the interface, there is an 'Apply' button.

## Example



In this example, you will configure port5 on *FortiGate Root* to be managed by FortiIPAM and specify the network size. Next you will enable DHCP on the interface to supply IP addresses to this network.

Once FortiIPAM is designated as the IP source, you will configure the port5 interface on *FortiGate Downstream* to obtain an IP from DHCP to connect it to *FortiGate Root* and add it to the Security Fabric. Lastly, you will use FortiIPAM to assign IP addresses to the *Internal Network*.

1. On *FortiGate Root*, edit port5 and configure the interface to be managed by FortiIPAM.
  - a. Go to *Network > Interfaces*, and double-click port5 to edit it. The *Edit Interface* window opens.
  - b. From the *Role* dropdown, select *LAN*.
  - c. In the *Addressing mode* area, select *Auto-managed by FortiIPAM*. An information icon appears next to *IP/Netmask* and below the *Network Size* dropdown indicating FortiIPAM will allocate an IP subnet with the selected size.
  - d. From the *Network Size* dropdown, select the size of the network segment for this interface.
  - e. Enable *DHCP Server* to allow the interface to supply IP addresses to this network. You do not need to configure *Address range* and *Netmask*. These will be configured by FortiIPAM.
  - f. Click *OK*. Port5 gets an IP address from FortiIPAM corresponding to the network size. It will also start assigning addresses through DHCP. Refresh this page if an IP has not been assigned.

**Edit Interface**

Name: port5  
 Alias:   
 Type: Physical Interface  
 Role: LAN

Addressing mode: Manual DHCP **Auto-managed by FortiIPAM** One-Arm Sniffer  
 IP/Netmask: 10.128.6.1/255.255.255.0 [Show Global IP Allocation Map](#)  
 Network size: 256 (255.255.255.0)  
 Create address object matching subnet: ☐

**Administrative access**

IPv4: ☒ HTTPS ☒ HTTP ☒ PING  
☐ FMG-Access ☒ SSH ☐ SNMP  
☐ FTM ☐ RADIUS Accounting ☒ Security Fabric Connection

Receive LLDP: ☒ Use VDOM Setting **Enable** Disable  
 Transmit LLDP: ☒ Use VDOM Setting **Enable** Disable

**DHCP Server**

Address range: 10.128.6.1-10.128.6.254  
 Netmask: 255.255.255.0  
 Default gateway: **Same as Interface IP** Specify  
 DNS server: **Same as System DNS** Same as Interface IP Specify  
 Lease time: 604800 second(s)

**Advanced**

Network  
 Device detection: ☒

Traffic Shaping  
 Outbound shaping profile: ☐

Miscellaneous  
 Comments:   
 Status: ☒ Enabled ☐ Disabled

OK Cancel

## 2. View the IP allocation map.

- Go to **Network > Interfaces**, and double-click port5 to view it.
- In the **IP/Netmask** area, click **Show Global IP Allocation Map**. You are redirected to FortiCloud.

Addressing mode: Manual DHCP **Auto-managed by FortiIPAM** One-Arm Sniffer  
 IP/Netmask: 10.128.6.1/255.255.255.0 [Show Global IP Allocation Map](#)  
 Network size: 256 (255.255.255.0)  
 Create address object matching subnet: ☐

- Click **Login**. The FortiIPAM portal opens. The **List View** displays the assigned IP entries.
- Double-click an IP entry and click the **Source** tab. The IP source appears in the **Device** column. The **Interface** column displays the port. **Assign Type** displays **Auto**. **Last Updated** displays the assign time.

**FortiCloud**

**FortiIPAM**

**Subnets & IP Addresses**

**ADD SUBNET**

**IP Networks**

Reported by FortiGate

- Class A
- Class B
- Class C
- New Group

**List View** Heatmap View

Rows per page: 10 1-1 of 1

Subnet	Source	Address	CIDR	Netmask	Conflict	IP #	DHCP Server #	FGT Interface #
10.128.6.0/24	FGT	10.128.6.0	24	255.255.255.0	No	256	0	1

Subnet: 10.128.6.0/24 IP Address: 10.128.6.0

**OVERVIEW** **SOURCE**

Source	Device	Interface	DHCP Server	Assign Type	Last Updated	Comment
FGT	FGVM000000000000	port5		Auto	29 Apr 2020, 10:47 am	

## 3. On FortiGate Root go to Network > Interfaces. The DHCP Server settings are configured automatically.

4. On *FortiGate Downstream*, configure port5 to obtain an IP from DHCP.
  - a. Go to *System > FortiGuard*, and verify FortiIPAM is licensed.
  - b. Go to *Network > Interfaces*, and double click port5 to edit it.
  - c. In the *Addressing mode* area, select *DHCP* and click *OK*. The interface will get its IP address from the DHCP server configured on *FortiGate Root*.
  - d. In *Network > Interfaces*, double-click port5. The following fields appear in the *Address* area:
    - *Status*.
    - *Obtained IP/Netmask*
    - *Expiry Date*
    - *Acquired DNS*

Address	
Addressing mode	Manual <b>DHCP</b> Auto-managed by FortiIPAM
Status	<b>Connected</b>
Obtained IP/Netmask	10.128.6.2 255.255.255.0 <a href="#">Renew</a>
Expiry Date	2020/05/06 11:10:10
Acquired DNS	172.16.95.140
Retrieve default gateway from server	<input type="checkbox"/>
Override internal DNS	<input type="checkbox"/>

5. Add *FortiGate Downstream* to the Security Fabric.
  - a. Go to *Security Fabric > Fabric Connectors*. In the *Security Fabric Settings* area, set *Status* to *Enabled*.
  - b. In the *Upstream FortiGate IP* field, enter the IP address for *FortiGate Root*, and click *OK*. The *Topology* pane shows the connection is established.

Core Network Security

Security Fabric Setup

Security Fabric Settings

Status

☒ Enabled
 ☐ Disabled

Security Fabric role

Upstream FortiGate IP

Allow other Security Fabric devices to join

☐

SAML Single Sign-On

☐

Management IP/FQDN

Management port

Topology

SAML SSO

Guides

[Configure SAML Single Sign-On in the Security Fabric](#)

Documentation

[Online Help](#)
[Video Tutorials](#)

6. On *FortiGate Downstream*, configure port6 to use FortiIPAM.
  - a. Go to *Network > Interfaces*. Double-click port6 to edit it.
  - b. From the *Role* dropdown, select *LAN*.
  - c. In the *Address mode* area, select *Auto-managed by FortiIPAM*.
  - d. From the *Network size* dropdown, select a different network size. In this example, the network size was increased to 512.

FortiOS 6.4.0 New Features Guide  
Fortinet Inc.

200

- e. Wait a while and then double-click port6. The *IP/Netmask* is auto-populated.
- f. Enable *DHCP Server* to allow the interface to supply IP addresses to this network.
7. Go back to the FortiPAM portal in FortiCloud.
  - a. The *List View* tab shows the IP addresses for the downstream FortiGate.
  - b. Select a subnet, and click the *Source* tab. The source details show that the IP is different from the root FortiGate, preventing conflicts.

Subnet	Source	Address	CIDR	Netmask	Conflict	IP #	DHCP Server #	FGT Interface #
10.128.6.0/24	FGT	10.128.6.0	24	255.255.255.0	No	256	0	2
10.128.8.0/23	FGT	10.128.8.0	23	255.255.254.0	No	512	0	1

Source	Device	Interface	DHCP Server	Assign Type	Last Updated	Comment
FGT	FGVMC	port6		Auto	29 Apr 2020, 11:29 am	

### To view the FortiPAM service details in the CLI:

Use the `diagnose` command to view the FortiPAM service information in FortiGate.

```
Root-E (global) # diagnose test update info
...
System contracts:
...
IPMC,Thu Apr 15 17:00:00 2021
```



You can also use the REST API to get the FortiPAM service information.

```
https://172.16.116.xxx/api/v2/monitor/license/status
... "fortipam_cloud": {
  "type": "live_cloud_service",
  "status": "licensed",
  "expires": 1618531200,
  "entitlement": "IPMC"
}
```

### To configure FortiPAM in the CLI:

1. On *FortiGate Root*, edit port5 and configure the interface to be managed by FortiPAM. Use `managed-subnetwork-size` to specify the network size of the network segment for this interface.

In this example, the network size 256.

```
config system interface
  edit "port5"
    set ip-managed-by-fortipam enable
    set managed-subnetwork-size 256
  next
end
```

2. On the same interface, enable DHCP server on this interface to supply IP addresses to this network.



No configuration is required unless you need to change the defaults.

```
config system dhcp server
  edit 1
    set interface "port5"
    set dhcp-settings-from-fortipam enable
  next
end
```

3. Once FortiPAM completes the address configuration, the configurations will appear as follows:

```
show system interface
...
edit "port5"
  set vdom "root"
  set ip 10.128.6.1 255.255.255.0
  set allowaccess ping https ssh http fabric
  set type physical
  set device-identification enable
  set lldp-transmission enable
  set role lan
  set snmp-index 5
  set ip-managed-by-fortipam enable
next
...
end
show system dhcp server
edit 1
  set dns-service default
  set default-gateway 10.128.6.1
  set netmask 255.255.255.0
```



```

    set interface "port5"
    config ip-range
        edit 1
            set start-ip 10.128.6.1
            set end-ip 10.128.6.254
        next
    end
    set dhcp-settings-from-fortiipam enable
    config exclude-range
        edit 1
            set start-ip 10.128.6.1
            set end-ip 10.128.6.1
        next
    end
end
next
end

```

4. On *FortiGate Downstream*, configure port5 to obtain an IP from DHCP.

```

config system interface
    edit "port5"
        set mode dhcp
    next
end

```

5. After the IP is assigned and the device is connected to *FortiGate Root*, add *FortiGate Downstream* to the Security Fabric.
6. Once *FortiGate Downstream* is connected to the Security Fabric, you can configure the port6 interface to use the FortiIPAM service as well.
7. On *FortiGate Downstream*, set the interface to be managed by the FortiIPAM service, and increase the `managed-subnetwork-size` value.

In this example, the network size was increased to 512.

```

config system interface
    edit "port5"
        set ip-managed-by-fortiipam enable
        set managed-subnetwork-size 512
    next
end

```

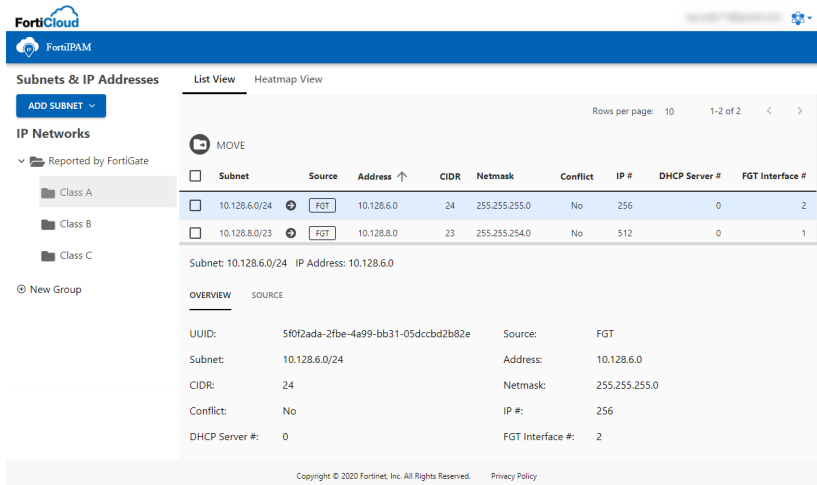
8. Configure the DHCP server on this port to assign IP addresses to this subnet.

```

config system dhcp server
    edit 1
        set interface "port6"
        set dhcp-settings-from-fortiipam enable
    next
end

```

9. Go to the FortiIPAM Portal to view the IP addresses.



**Subnets & IP Addresses** List View Heatmap View

ADD SUBNET

IP Networks

Reported by FortiGate

- Class A
- Class B
- Class C
- New Group

Subnet	Source	Address	CIDR	Netmask	Conflict	IP #	DHCP Server #	FGT Interface #
10.128.6.0/24	FGT	10.128.6.0	24	255.255.255.0	No	256	0	2
10.128.8.0/23	FGT	10.128.8.0	23	255.255.254.0	No	512	0	1

Subnet: 10.128.6.0/24 IP Address: 10.128.6.0

**OVERVIEW** SOURCE

UUID: 5f0f2ada-2fbc-4a99-bb31-05dccb2b82e Source: FGT

Subnet: 10.128.6.0/24 Address: 10.128.6.0

CIDR: 24 Netmask: 255.255.255.0

Conflict: No IP #: 256

DHCP Server #: 0 FGT Interface #: 2

Copyright © 2020 Fortinet, Inc. All Rights Reserved. Privacy Policy

## VRF GUI support - 6.4.2

From the *Network > Interfaces* page, users can configure virtual routing and forwarding (VRF) IDs directly on the interface. The VRF IDs can be displayed in the routing monitor and can be used to create blackhole static routes.

VRF allows multiple routing table instances to co-exist on the same router. One or more interfaces may have a VRF, and packets are only forwarded between interfaces with the same VRF.



Enable *Advanced Routing* in *System > Feature Visibility* to use this feature.

### To configure a VRF ID in the GUI:

1. Configure the interface:
  - a. Go to *Network > Interfaces* and click *Create New > Interface*.
  - b. Enter a value in the VRF ID field.
  - c. Configure the other settings as needed.

## d. Click OK.

e. To add the VRF column in the interface table, click the gear icon, select *VRF*, and click *Apply*.

Name	VRF	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges
dmz	0	Physical Interface		10.10.10.1/255.255.255.0		PING HTTPS HTTP FMG-Access		2.2.2.3-2.2.2.254
ha1	27	Physical Interface		0.0.0.0/0.0.0.0				
ha2	0	Physical Interface		0.0.0.0/0.0.0.0				
mgmt	0	Physical Interface		192.168.1.99/255.255.255.0		PING HTTPS SSH HTTP FMG-Access		192.168.1.110-192.168.1.210
port12	12	Physical Interface		188.10.22.1/255.255.255.0		PING HTTPS SSH SNMP		
port3	0	Physical Interface		0.0.0.0/0.0.0.0				
VLAN103 (test_interface)	14	VLAN		10.1.22.1/255.255.255.0		PING HTTPS SSH SNMP		10.1.22.2-10.1.22.254
port7	0	Physical Interface		0.0.0.0/0.0.0.0				
wan1	10	Physical Interface		172.27.5.61/255.255.255.0		PING HTTPS SSH SNMP		

## 2. Add a blackhole static route using the VRF ID:

- Go to *Network > Static Routes* and click *Create New*.
- Enter the subnet.
- In the *Interface* field, select *Blackhole*.
- In the *VRF ID* field, enter the ID you created in step 1.

## e. Click OK.

**To configure a VRF ID in the CLI:**

## 1. Configure the interface:

```
config system interface
    edit test_interface
        ...
        set vrf 14
    next
end
```

## 2. Add a blackhole static route using the VRF ID:

```
config router static
    edit 3
        set dst 8.8.8.8 255.255.255.255
        set blackhole enable
        set vrf 14
    next
end
```

**Determine if recursive distance is evaluated in BGP's next hops under ECMP - 6.4.2**

For BGP ECMP routes that require recursive lookup to the next hop, by default the routes are installed to the kernel, regardless of the distance to the next hop.

When the multipath recursive distance option is enabled, only the routes with the lowest recursive distance are installed. For example, a next hop that is recursively resolved by a connected router will be installed, but a next hop that is resolved by a static route will not, because its distance is higher.

**To enable the multipath recursive distance option:**

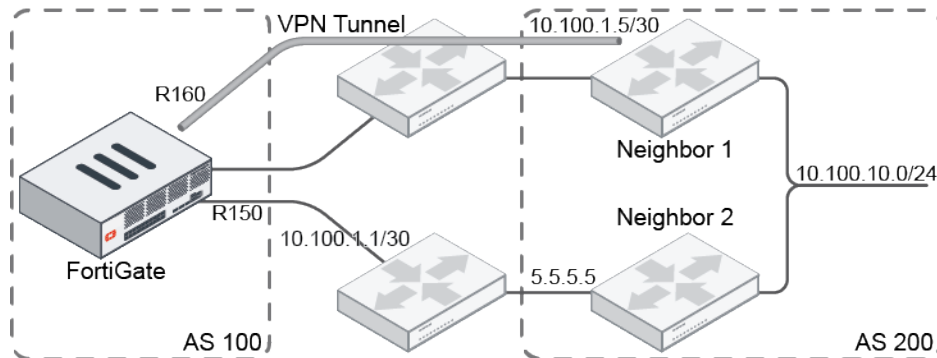
```
config router bgp
    set multipath-recursive-distance enable
end
```



Either EGBP or IGBP multipath must be enabled:

```
config router bgp
    set ebgp-multipath enable
    set ibgp-multipath enable
end
```

## Example



In this example, BGP has learned one BGP route from two neighbors with different next hops. One of the next hops is directly connected, so its recursive distance is zero. The other next hop is learned from a static route, so its recursive distance is higher.

When multipath recursive distance is disabled, all of the next hop routes are installed to the kernel and used to form the ECMP routes (default):

```
# get router info routing-table bgp
Routing table for VRF=0
B      10.100.10.0/24 [20/0] via 5.5.5.5 (recursive via 10.100.1.1, R150), 00:00:03
                                [20/0] via 10.100.1.5 (recursive is directly connected, R160),
00:00:03
B      10.100.11.0/24 [20/0] via 5.5.5.5 (recursive via 10.100.1.1, R150), 00:00:03
                                [20/0] via 10.100.1.5 (recursive is directly connected, R160),
00:00:03
```

When multipath recursive distance is enabled, only the shortest next hop route is installed to the kernel and used to form the ECMP routes:

```
# get router info routing-table bgp
Routing table for VRF=0
B      10.100.10.0/24 [20/0] via 10.100.1.5 (recursive is directly connected, R160),
00:00:39
B      10.100.11.0/24 [20/0] via 10.100.1.5 (recursive is directly connected, R160),
00:00:39
```

## PRP on SoC4 models - 6.4.3

Starting in 6.4.3, a PRP trailer header can be kept after passing through SoC4 model FortiGates in transparent mode.

### To configure PRP:

#### 1. Enable PRP:

```
config system settings
    set prp-trailer-action enable
end
```

**2. Configure the PRP ports:**

```
config system npu
    set prp-port-in <ingress port>
    set prp-port-out <egress port>
end
```

**Testing results summary:**

Model	Version and mode				Commands to enable PRP options
	6.2 TP	6.2 NAT	6.4 TP	6.4 NAT	
SoC4	No	No	Pass	No	config system settings config system npu-setting prp
NP6	No	No	No	No	Not supported
NP7	Pass	No	-	-	config system settings
Non-NP platform	Pass	No	-	-	config system settings
VM64	Pass	No	Pass	No	config system settings

**FN-TRAN-DSL module on FG-80F and FGR-60F-3G4G - 6.4.9**

Administrators can maintain multiple ISP circuits on a single FortiGate using the `sfp-dsl` command. This implements an all-in-one solution that uses less power supply cords, less cabling, and avoids unreliable ISP modems.

The `sfp-dsl` command can enable or disable DSL functions on the SFP transceiver interface. The interface acts as a regular port when the command is disabled.

```
config system interface
    edit <port>
        set phy-mode {adsl | vdsl}
        set tc-mode {ptm | atm}
        set retransmission {enable | disable}
        set vectoring {enable | disable}
        set sfp-dsl {enable | disable}
        set sfp-dsl-autodetect {enable | disable}
        set sfp-dsl-adsl-fallback {enable | disable}
    next
end
```

`phy-mode {adsl | vdsl}` Set the DSL physical mode:

- `adsl`: use ADSL
- `vdsl`: use VDSL

`tc-mode {ptm | atm}` Set the DSL transfer mode:

- `ptm`: use PTM
- `atm`: use ATM

retransmission {enable   disable}	Enable/disable DSL retransmission.
vectoring {enable   disable}	Enable/disable DSL vectoring.
sfp-dsl {enable   disable}	Enable/disable SFP DSL.
sfp-dsl-autodetect {enable   disable}	Enable/disable SFP DSL MAC address autodetect.
sfp-dsl-adsl-fallback {enable   disable}	Enable/disable DSL ADSL fallback.

### To configure DSI functions on the SFP transceiver interface:

```

config system interface
    edit "wan1"
        set vdom "root"
        set mode pppoe
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
fabric ftm dnp
    set type physical
    set phy-mode vdsl
    set tc-mode ptm
    set sfp-dsl enable
    set role wan
    set snmp-index 1
    set username "pc01"
    set password *****
next
end

```



The interface mode can be configured to DHCP or PPPoE.

### To retrieve SFP modular information:

```

# get system interface transceiver
Interface wan1 - SFP/SFP+ (1.3G)
  Vendor Name   : FORTINET
  Part No.      : FN-TRAN-DSL
  Serial No.    : 18234K86A2000000
  SFP-DSL MAC   : 00:03:79:07:14:CD
Interface wan2 - Transceiver is not detected.

```

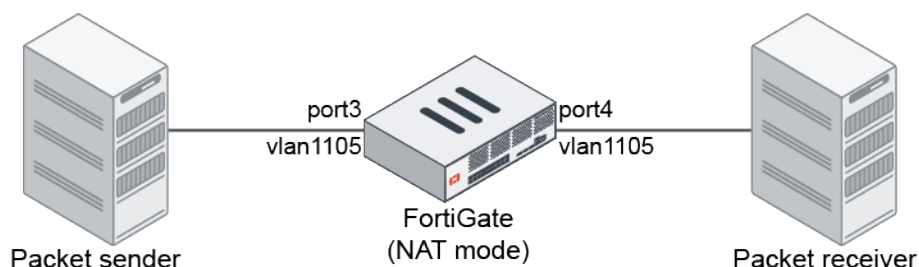
SFP/SFP+	Temperature	Voltage	Optical Tx Bias	Optical Tx Power	Optical Rx Power
Interface	(Celsius)	(Volts)	(mA)	(dBm)	(dBm)
wan1	N/A	N/A	N/A	N/A	N/A

++ : high alarm, + : high warning, - : low warning, -- : low alarm, ? : suspect.

## Reset the VLAN DEI bit when passing through a FortiGate in NAT mode - 6.4.9

When a FortiGate is in NAT mode, a VLAN tag with a Drop Eligible Indicator (DEI, formerly CFI or Canonical Format Indicator) bit set is reset to 0 after passing through the FortiGate. In transparent mode or when passing through a virtual wire pair, the DEI bit is not changed.

### Topology



### Example 1

In this example, when there incoming traffic coming to port3, its VLAN DEI is 1. When traffic egresses on port4, the DEI bit is reset to 0.

#### To verify the DEI bits:

##### 1. Sniff the traffic on port3:

```
# diagnose sniffer packet port3 "" 6

129.698250 port3 -- 802.1Q vlan#1105 P7
0x0000 704c a553 1954 0010 9411 0001 8100 f451 pL.S.T.....Q
0x0010 0800 45c0 006a 0006 0000 ff11 b4b6 0101 ..E..j.....
0x0020 0102 0202 0202 0400 0400 0056 b4be 0000 .....V....
0x0030 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0040 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0050 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0060 0000 0000 0000 0000 9313 aa44 52c1 90e3 .....DR...
0x0070 dlec dcb0 6c0b 4301 84cc 3909 ....l.C...9.
```

##### 2. Sniff the traffic on port4:

```
# diagnose sniffer packet port4 "" 6

42.935025 port4 -- 802.1Q vlan#1105 P7
0x0000 0010 9422 0002 704c a553 1955 8100 e451 ...".pL.S.U...Q
0x0010 0800 45c0 006a 0008 0000 fe11 b5b4 0101 ..E..j.....
0x0020 0102 0202 0202 0400 0400 0056 852a 0000 .....V.*..
0x0030 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0040 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0050 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0060 0000 0000 0000 0000 91f0 161d e232 159c .....2..
0x0070 4649 d361 e01b 89a2 3e48 0a83 FI.a....>H..
```

The DEI changed from f451 to e451, so it was cleared and reset to 0.



## Example 2

In this example, when there incoming traffic coming to port3, its VLAN DEI is 0. The egress traffic on port4 still keeps the DEI bit as 0.

### To verify the DEI bits:

#### 1. Sniff the traffic on port3:

```
# diagnose sniffer packet port3 "" 6

194.457945 port3 -- 802.1Q vlan#1105 P7
0x0000 704c a553 1954 0010 9411 0001 8100 e451 pL.S.T.....Q
0x0010 0800 45c0 006a 0008 0000 ff11 b4b4 0101 ..E..j.....
0x0020 0102 0202 0202 0400 0400 0056 852a 0000 .....V.*..
0x0030 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0040 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0050 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0060 0000 0000 0000 0000 88a4 7d05 c787 2161 .....}...!a
0x0070 8abf 88c9 496f 635f 90b4 2c72 ....Ioc_...r
```

#### 2. Sniff the traffic on port4:

```
# diagnose sniffer packet port4 "" 6

192.457951 port4 -- 802.1Q vlan#1105 P7
0x0000 0010 9422 0002 704c a553 1955 8100 e451 ..."..pL.S.U...Q
0x0010 0800 45c0 006a 0008 0000 fe11 b5b4 0101 ..E..j.....
0x0020 0102 0202 0202 0400 0400 0056 852a 0000 .....V.*..
0x0030 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0040 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0050 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0060 0000 0000 0000 0000 88a4 7d05 c787 2161 .....}...!a
0x0070 8abf 88c9 496f 635f 90b4 2c72 ....Ioc_...r
```

The DEI is the same (e451), so it is not cleared and remains as 0.

## FS-TRANS-FX module on FGR-60F and FGR-60F-3G4G - 6.4.9

FS-TRAN-FX 100 Mbps SFP optical transceivers are supported on FGR-60F and FGR-60F-3G4G devices.

The interface speed must be set to 100full or 100half.

```
config system interface
    edit <name>
        set speed {100full | 100half}
    next
end
```

In this example, wan1 is an SFP1 interface, and wan2 is an SFP2 interface.

### To verify that the transceiver ports are working:

```
# get system interface transceiver
Interface wan1 - SFP/SFP+ (0.2G)
Vendor Name   : Optech
```

```

Part No.      : OP6A-M02-13-IM
Serial No.    : L205050000
SFP-DSL MAC   : Interface wan2 - SFP/SFP+ (0.2G)
Vendor Name   : Optech
Part No.      : OP6A-M02-13-IM
Serial No.    : L205050000
SFP-DSL MAC   :

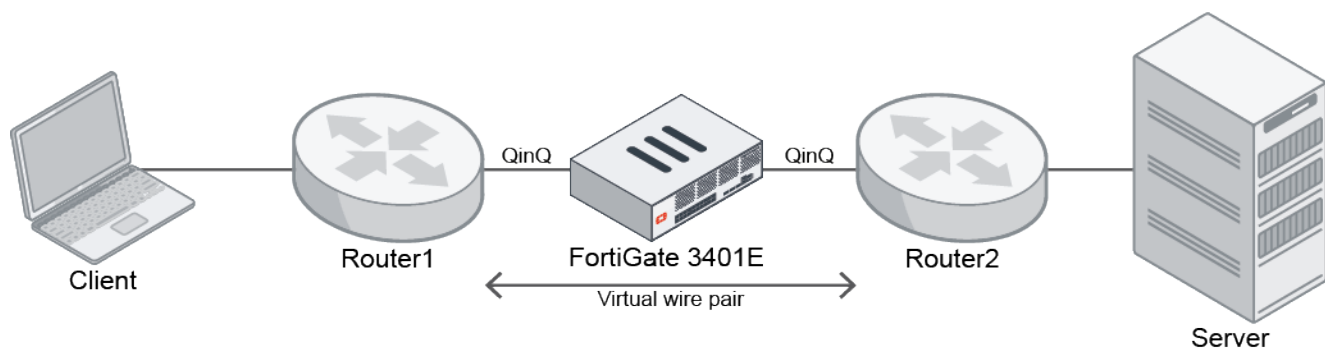
```

SFP/SFP+ Interface	Temperature (Celsius)	Voltage (Volts)	Optical Tx Bias (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)
wan1	36.2	3.29	11.56	-15.7	-16.0
wan2	36.6	3.30	12.41	-16.0	-17.5

++ : high alarm, + : high warning, - : low warning, -- : low alarm, ? : suspect.

## Inspect double-tagged traffic on virtual wire pairs - 6.4.9

Double-tagged (802.1Q and 802.1Q) traffic can be inspected on a virtual wire pair with wildcard VLANs. The NPU has been optimized to receive packet steering and configure traffic distribution on the Integrated Switch Fabric (ISF) to achieve higher throughput. This feature is supported on FG-3400E, FG-3401E, FG-3600E, and FG-3601E models.



In this example, the FortiGate interfaces are part of a virtual wire pair. The FortiGate receives packets that are double-tagged with two 802.1Q tags with 0x8100 frames. A virtual wire pair policy using wildcard VLANs is able to inspect the payload within the internal tag.

Affinity fine-tuning, also known as receive packet steering (RPS) can be configured. This fine-tuning allows users to configure the interface receive queue mapping to different CPU cores, which evenly distributes packets among different cores and improves performance.

```

config system affinity-packet-redistribution
    edit <id>
        set interface <string>
        set rxqid <integer>
        set affinity-cpumask <hexadecimal>
    next
end

```

interface <string>	Enter the name of the physical interface to perform packet redistribution on.
rxqid <integer>	Enter the ID of the receive queue (when the interface has multiple queues) to perform packet redistribution on.

```
affinity-cpumask
    <hexadecimal>
```

Enter the affinity setting for VM throughput (64-bit hexadecimal value, 0XXXXXXXXXXXXXXXXX).

Packet distribution is allowed to occur on the ISF using a round-robin algorithm to get higher throughput.

```
config system npu
    set isf-np-rx-tr-distr {port-flow | round-robin | randomized}
    set rps-mode {enable | disable}
end
```

```
isf-np-rx-tr-distr {port-
    flow | round-robin |
    randomized}
```

Set the traffic distribution type in the ISF:

- port-flow: enhanced hashing
- round-robin: round-robin member selection
- randomized: randomized load balancing mode

```
rps-mode {enable |
    disable}
```

Enable/disable NPU receive packet steering (RPS) optimization mode.

## Support 802.1X on virtual switch for certain NP6 platforms - 6.4.10

802.1X is supported under the hardware switch interface on the following NP6 platforms: FG-30xE, FG-40xE, and FG-110xE.

For more information about this feature, see [Support 802.1X on virtual switch for certain NP6 platforms](#).

## IPv6

This section includes information about IPv6 related new features:

- [IPv6 geography-based address support on page 213](#)
- [Support for IPv6 in central SNAT table on page 215](#)
- [FQDN support for remote gateways on page 217](#)
- [MAP-E support 6.4.1 on page 219](#)
- [IPv6 MAC addresses and usage in firewall policies 6.4.2 on page 223](#)

### IPv6 geography-based address support

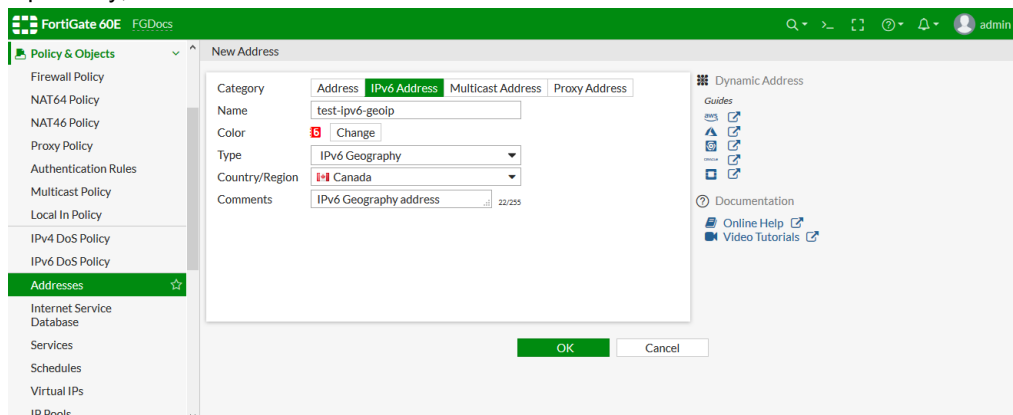
Geography-based IPv6 addresses can be created and applied to IPv6 firewall policies.



IPv6 geography-based addresses do not support `geoip-override` or `geoip-anycast`.

### To create an IPv6 geography-based address in the GUI:

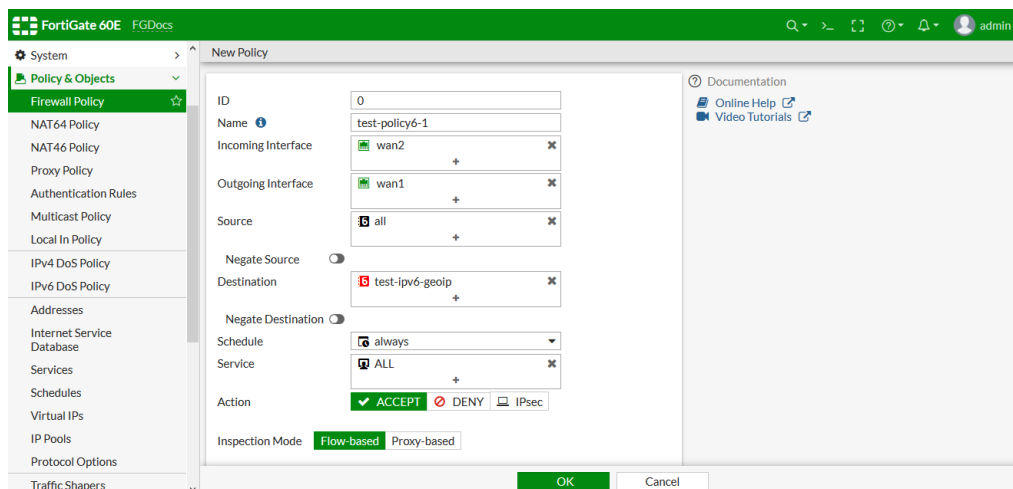
1. Go to *Policy and Objects > Addresses*.
2. Click *Create New > Address*.
3. Set *Category* to *IPv6 Address*.
4. Enter a name for the address.
5. Set *Type* to *IPv6 Geography*.
6. Select the *Country/Region* from the list.
7. Optionally, enter comments.



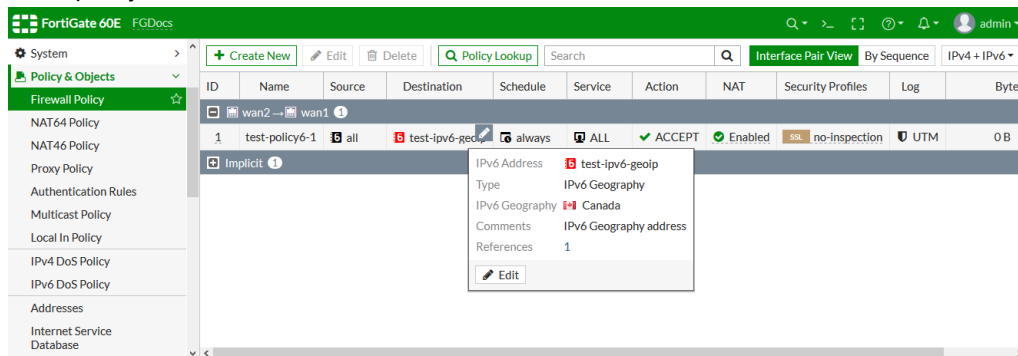
8. Click *OK*.

### To use the IPv6 geography address in a policy:

1. Go to *Policy & Objects > Firewall Policy*.
2. Edit an existing policy, or create a new one, using the IPv6 geography address as the *Source* or *Destination Address*.



3. In the policy list, hover over the address to view details.



### To configure an IPv6 geography-based address in the CLI:

1. Create an IPv6 geography-based address:

```
config firewall address6
    edit "test-ipv6-geoip"
        set type geography
        set color 6
        set comment "IPv6 Geography address"
        set country "CA"
    next
end
```

2. Use the IPv6 geography-based address in a policy:

```
config firewall policy
    edit 1
        set name "test-policy6-1"
        set srcintf "wan2"
        set dstintf "wan1"
        set srcaddr6 "all"
        set dstaddr6 "test-ipv6-geoip"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

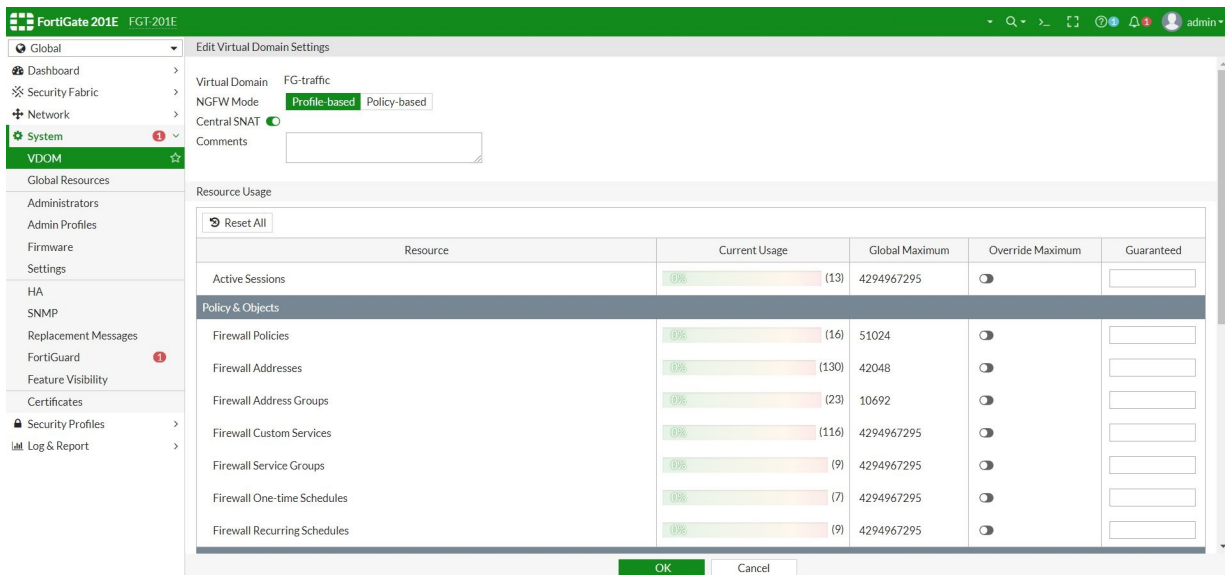
## Support for IPv6 in central SNAT table

IPv4 and IPv6 central SNAT maps are displayed in the same table.

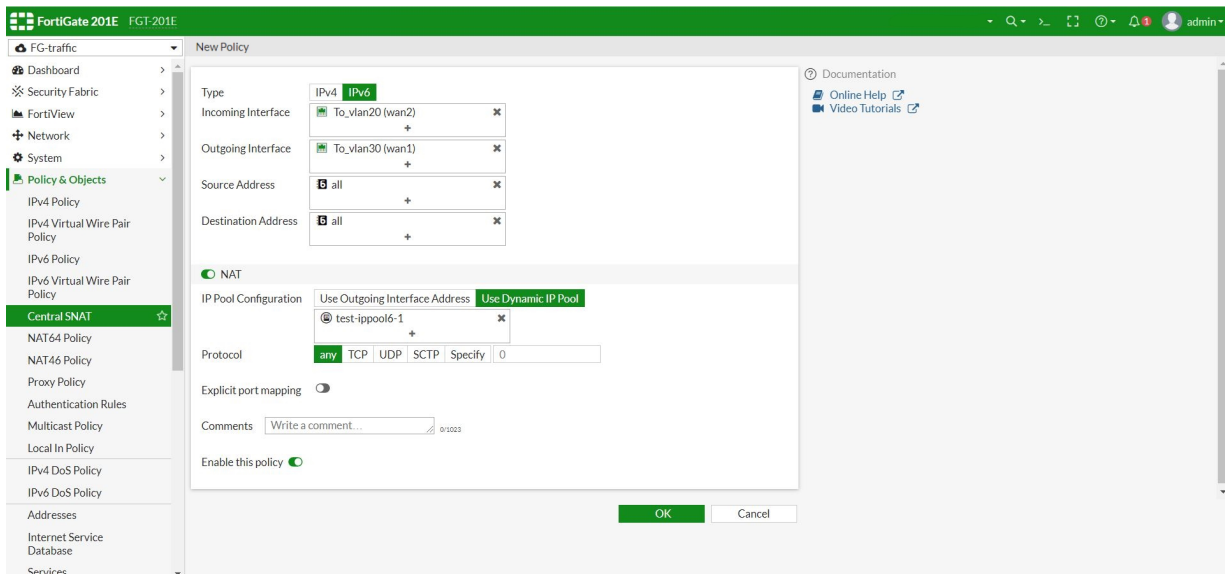
### To configure an IPv6 policy with central SNAT in the GUI:

1. Enable central SNAT:
  - a. In the Global VDOM, go to *System > VDOM*.
  - b. Select a VDOM and click *Edit*. The *Edit Virtual Domain Settings* pane opens.
  - c. Enable *Central SNAT*.

d. Click OK.



2. Go in to the VDOM with central SNAT enabled (FG-traffic in this example).
3. Go *Policy & Objects > Central SNAT* and click *Create New*.
4. Configure the policy settings:
  - a. For *Type*, select *IPv6*.
  - b. Enter the interface, address, and IP pool information.
  - c. Configure the other settings as needed.
  - d. Click OK.



The matching SNAT traffic will be handled by the IPv6 central SNAT map.

## To configure an IPv6 policy with central SNAT in the CLI:

### 1. Enable central SNAT:

```
config vdom
    edit FG-traffic
        config system settings
            set central-nat enable
        end
    next
end
```

### 2. Create an IPv6 central SNAT policy:

```
config vdom
    edit FG-traffic
        config firewall central-snat-map
            edit 2
                set type ipv6
                set srcintf "wan2"
                set dstintf "wan1"
                set orig-addr6 "all"
                set dst-addr6 "all"
                set nat-ippool6 "test-ippool6-1"
            next
        end
    next
end
```

### 3. Verify the SNAT traffic:

```
(FG-traffic) # diagnose sniffer packet any icmp6 4
interfaces=[any]
filters=[icmp6]
3.602891 wan2 in 2000:10:1:100::41 -> 2000:172:16:200::55: icmp6: echo request seq 0
3.602942 wan1 out 2000:172:16:200::199 -> 2000:172:16:200::55: icmp6: echo request seq 0
3.603236 wan1 in 2000:172:16:200::55 -> 2000:172:16:200::199: icmp6: echo reply seq 0
3.603249 wan2 out 2000:172:16:200::55 -> 2000:10:1:100::41: icmp6: echo reply seq 0
4.602559 wan2 in 2000:10:1:100::41 -> 2000:172:16:200::55: icmp6: echo request seq 1
4.602575 wan1 out 2000:172:16:200::199 -> 2000:172:16:200::55: icmp6: echo request seq 1
4.602956 wan1 in 2000:172:16:200::55 -> 2000:172:16:200::199: icmp6: echo reply seq 1
4.602964 wan2 out 2000:172:16:200::55 -> 2000:10:1:100::41: icmp6: echo reply seq 1
^C
8 packets received by filter
0 packets dropped by kernel
```

## FQDN support for remote gateways

FortiGate supports FQDN when defining an IPsec remote gateway with a dynamically assigned IPv6 address. When FortiGate attempts to connect to the IPv6 device, FQDN will resolve the IPv6 address even when the address changes.

Using FQDN to configure the remote gateway is useful when the remote end has a dynamic IPv6 address assigned by their ISP or DHCPv6 server.

### 1. Set the VPN to DDNS and configure FQDN

```
config vpn ipsec phase1-interface
```

```

edit "ddns6"
    set type ddns
    set interface "agg1"
    set ip-version 6
    set ike-version 2
    set peertype any
    set net-device disable
    set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
        chacha20poly1305-prfsha256
    set dpd on-idle
    set remotegw-ddns "rgwa61.vpnlab.org"
    set psksecret xxxxxxxx
next
end
config vpn ipsec phase2-interface
    edit "ddns6"
        set phaselname "ddns6"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
            chacha20poly1305
        set src-addr-type subnet6
        set dst-addr-type subnet6
        set src-subnet6 2003:1:1:1::/64
    next
end

```

## 2. FQDN resolves the IPv6 address

```

# diagnose test application dnsproxy 7
vfid=0, name=rgwa61.vpnlab.org, ttl=3600:3547:1747
2003:33:1:1:22 (ttl=3600)

```

## 3. FortiGate uses FQDN to connect to the IPv6 device

```

# diagnose vpn tunnel list name ddns6
list ipsec tunnel by names in vd 0

-----

name=ddns6 ver=2 serial=2 2003:33:1:1:1:0->2003:33:1:1:22:0 dst_mtu=1500
bound_if=32 lgwy=static/1 tun=intf/0 mode=auto/1 encaps=none/520 options[0208]=npu frag-rfc
    run_state=0 accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=10 ilast=9 olast=9 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=72340
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=ddns6 proto=0 sa=1 ref=2 serial=1
    src: 0:2003:1:1:1:1::/64:0
    dst: 0:::0:0
    SA: ref=3 options=10226 type=00 soft=0 mtu=1422 expire=42680/0B replaywin=2048
        seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
    life: type=01 bytes=0/0 timeout=42901/43200
    dec: spi=ac7a5718 esp=aes key=16 9976b66280cc49f500d8edca093e03fb
        ah=sha1 key=20 4d94d76fc18df5a180c52e0a6cd5f430fde48fe8
    enc: spi=7ab888ec esp=aes key=16 841a95d3ee5ea5108a2ba269b74998d1
        ah=sha1 key=20 ed0b52d27776e30149ee36af4fd4626681c2a3a1
    dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
    npu_flag=00 npu_rgwy=2003:33:1:1:22 npu_lgwy=2003:33:1:1:1 npu_selid=0 dec_npuuid=0 enc_
        npuid=0

```



```
run_tally=1
```

#### 4. The tunnel can still connect to the FQDN address when the IPv6 address changes

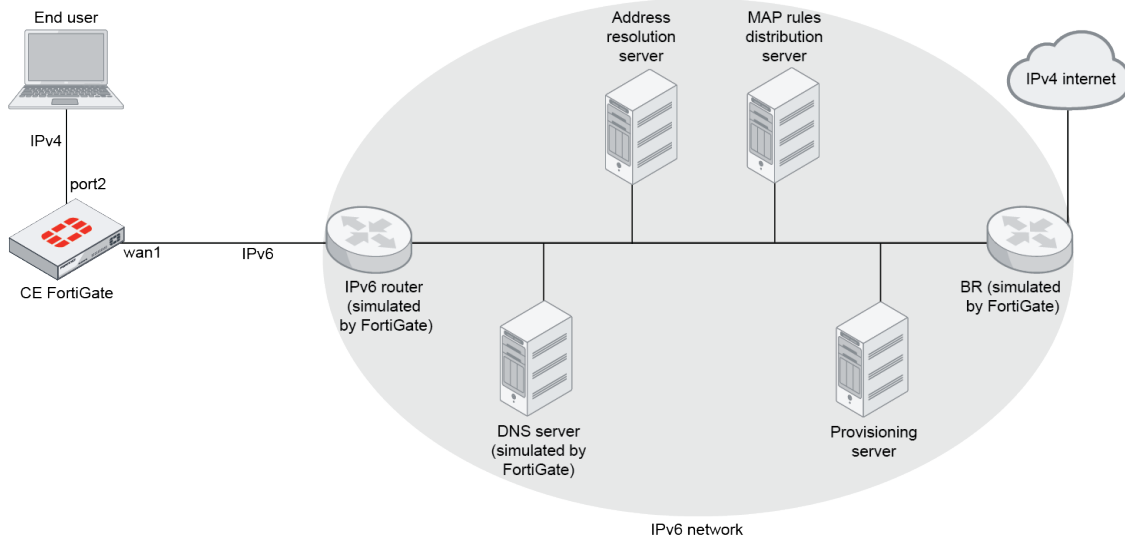
```
# diagnose debug application ike -1
# diagnose debug enable
ike 0:ddns6: set oper down
ike 0:ddns6: carrier down
ike shrank heap by 159744 bytes
ike 0: cache rebuild start
ike 0:ddns6: sending DNS request for remote peer rgwa61.vpnlab.org
ike 0: send IPv6 DNS query : rgwa61.vpnlab.org
ike 0: cache rebuild done
ike 0:ddns6: remote IPv6 DDNS gateway is empty, retry to resolve it
ike 0: DNS response received for remote gateway rgwa61.vpnlab.org
ike 0: DNS rgwa61.vpnlab.org -> 2003:33:1:1::33
ike 2:test:46932: could not send IKE Packet(P1_RETRANSMIT):50.1.1.1:500->50.1.1.2:500,
    len=716: error 101:Network is unreachable
ike 0:ddns6: remote IPv6 DDNS gateway is empty, retry to resolve it
ike 0:ddns6: 'rgwa61.vpnlab.org' resolved to 2003:33:1:1::33
ike 0: cache rebuild start
ike 0:ddns6: local:2003:33:1:1::1, remote:2003:33:1:1::33
ike 0:ddns6: cached as static-ddns.
ike 0: cache rebuild done
ike 0:ddns6: auto-negotiate connection
ike 0:ddns6: created connection: 0x155aa510 32 2003:33:1:1::1->2003:33:1:1::33:500.

.....

ike 0:ddns6:46933:ddn6:47779: add IPsec SA: SPIs=ac7a5719/7ab888ed
ike 0:ddns6:46933:ddn6:47779: IPsec SA dec spi ac7a5719 key
    16:0F27F1D1D02496F90D15A30E2C032678 auth 20:46564E0E86A054374B31E58F95E4458340121BCE
ike 0:ddns6:46933:ddn6:47779: IPsec SA enc spi 7ab888ed key
    16:926B12908EE670E1A5DDA6AD8E96607B auth 20:42BF438DC90867B837B0490EAB08E329AB62CBE3
ike 0:ddns6:46933:ddn6:47779: added IPsec SA: SPIs=ac7a5719/7ab888ed
ike 0:ddns6:46933:ddn6:47779: sending SNMP tunnel UP trap
ike 0:ddns6: carrier up
```

## MAP-E support - 6.4.1

On a customer edge (CE) FortiGate, an IPv4-over-IPv6 (MAP-E) tunnel can be created between the FortiGate and the border relay (BR) operating in an IPv6 network. A tunnel interface is created between the FortiGate and BR, which can be applied to firewall policies and IPsec VPN.



### To configure a MAP-E tunnel between the FortiGate and the BR:

1. Configure fixed IP mode.
  - a. Configure IPv6 on the interface:

```
config system interface
  edit "wan1"
    config ipv6
      set autoconf enable
      set unique-autoconf-addr enable
      set interface-identifier ::6f:6clf:3400:0
    end
  next
end
```

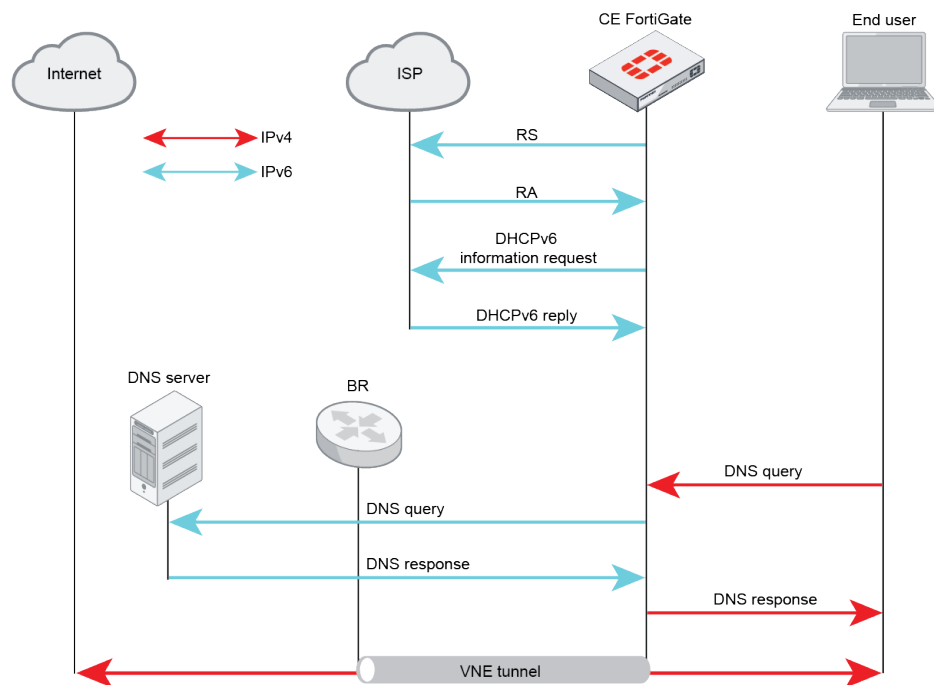
The `interface-identifier` is an IPv6 address. Its last 64-bit will be kept and the rest will be cleared automatically. It will combine with the IPv6 prefix it gets from the IPv6 router to generate the IPv6 address of the interface.

By default, `unique-autoconf-addr` is disabled. It must be enabled so it can handle IPv6 prefix changing.

- b. Configure the VNE tunnel:

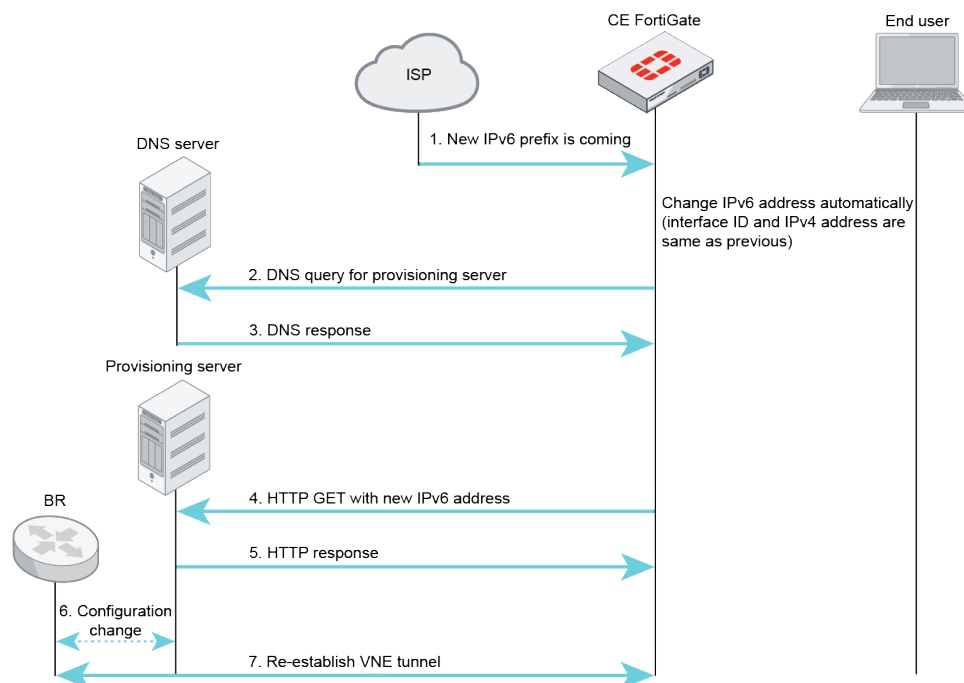
```
config system vne-tunnel
  set status enable
  set interface "wan1"
  set mode fixed-ip
  set ipv4-address 10.10.81.81 255.255.255.0
  set br 2001:160::82
  set update-url "http://qa.forosqa.com/update?user=xxxx&pass=yyyy"
end
```

Initial sequence overview of VNE tunnel under fixed IP mode:



Once the IPv6 address of the FortiGate changes, the tunnel will be down because the BR does not know the FortiGate's new IPv6 address. The FortiGate uses `update-url` to update the new IPv6 address to the provisioning server. The provisioning server updates the FortiGate's IPv6 address to the BR so the VNE tunnel can be re-established.

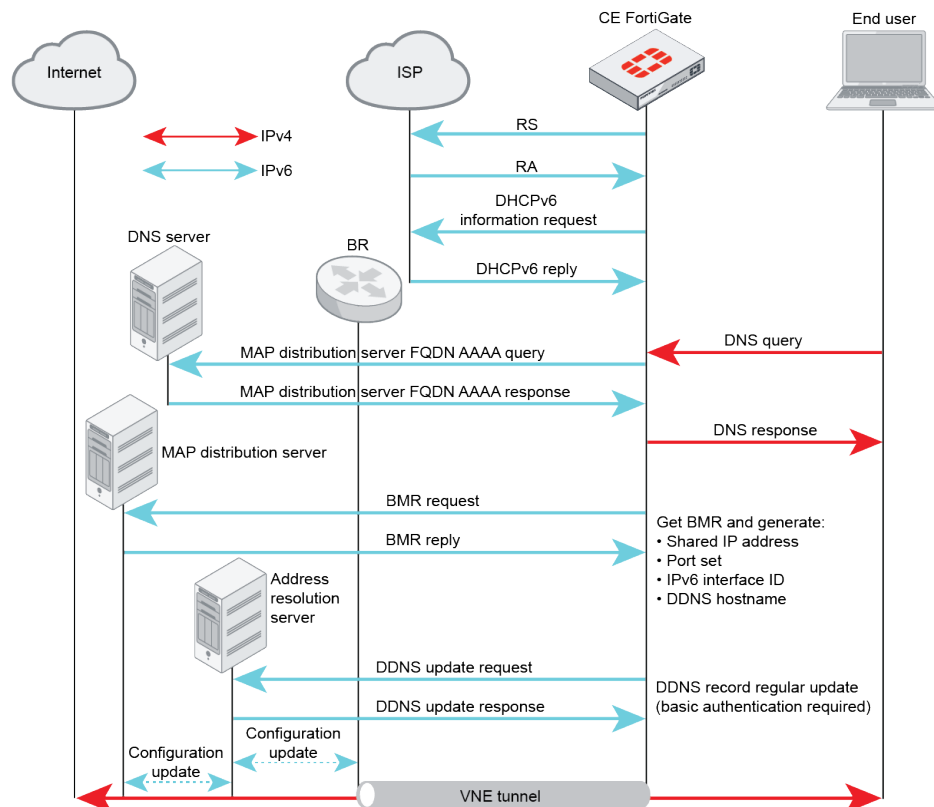
Communication sequence overview of re-establishing VNE tunnel:



## 2. Configure the VNE tunnel to use MAP-E mode:

```
config system vne-tunnel
  set status enable
  set interface 'wan1'
  set ssl-certificate "Fortinet_Factory"
  set bmr-hostname *****
  set auto-asic-offload enable
  set mode map-e
end
```

### Initial sequence overview of VNE tunnel under MAP-E mode:



The FortiGate sends a MAP rule request to the MAP distribution server once the IPv6 address is configured on the FortiGate by RS/RA. Next, the FortiGate will send an AAAA query to get the IPv6 address of the MAP distribution server. After sending the BMR request to the MAP distribution server, the FortiGate will get the IPv4 address, port set, BR IPv6 address, and hostname of the address resolution server from the BMR reply. The VNE tunnel between the FortiGate and BR is now established.

The address resolution server is actually a dynamic DNS. The hostname is used for the FortiGate to maintain an IPv6 address when it changes.

The FortiGate updates the DDNS server with its IPv6 address whenever it updates, which in turn provides the update to the MAP distribution server and BR so they know how to resolve the FortiGate by hostname.

Once the VNE tunnel is established, a tunnel interface is created (`vne.root`), and an IPv4-over-IPv6 tunnel is set up between the FortiGate and BR. The route, firewall policy, and DNS server can now be configured to let the traffic go through the VNE tunnel and protect the end-user. The VNE tunnel can also be used in IPsec phase 1.

**3. Configure the route:**

```
config router static
  edit 1
    set device "vne.root"
  next
end
```

**4. Configure the firewall policy:**

```
config firewall policy
  edit 111
    set name "ff"
    set srcintf "port2"
    set dstintf "vne.root"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set ssl-ssh-profile "certificate-inspection"
    set av-profile "default"
    set nat enable
  next
end
```

**5. Configure the DNS server:**

```
config system dns-server
  edit "port2"
  next
end
```

## IPv6 MAC addresses and usage in firewall policies - 6.4.2

Users can define IPv6 MAC addresses that can be applied to the following policies:

- Firewall
- Virtual wire pair
- ACL/DoS
- Central NAT
- NAT64
- Local-in

In this example, a firewall policy is configured in a NAT mode VDOM with the IPv6 MAC address range as a source address.



IPv6 MAC addresses cannot be used as destination addresses in VDOMs when in NAT operation mode.

---

## To configure IPv6 MAC addresses in a policy in the GUI:

1. Create the MAC address range:
  - a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
  - b. For *Category*, click *IPv6 Address*.
  - c. Enter an address name.
  - d. For *Type*, select *Device (MAC Address)*.
  - e. For *MAC Address Scope*, click *Range*.
  - f. Enter the *Starting* and *Ending* MAC addresses.
  - g. Click *OK*.

2. Configure the policy:
  - a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
  - b. For *Source*, select the IPv6 MAC address object.
  - c. Configure the other settings as needed.
  - d. Click *OK*.

**To configure IPv6 MAC addresses in a policy in the CLI:****1. Create the MAC address range:**

```
config firewall address6
    edit "test-ipv6-mac-addr-1"
        set type mac
        set start-mac 00:0c:29:b5:92:8d
        set end-mac 00:0c:29:b5:92:8d
    next
end
```

**2. Configure the policy:**

```
config firewall policy
    edit 2
        set srcintf "wan2"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "test-ipv6-mac-addr-1" "2000-10-1-100-0"
        set dstaddr6 "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end
```

## Web proxy

This section includes information about web proxy related new features:

- [Authentication support for upstream proxy in transparent proxy mode on page 225](#)
- [Support TLS 1.3 for proxy forward servers in certificate inspection mode 6.4.1 on page 227](#)

### Authentication support for upstream proxy in transparent proxy mode

A downstream proxy FortiGate that needs to be authenticated by the upstream web proxy can use the basic authentication method to send its username and password, in the base64 format, to the upstream web proxy for authentication. If the authentication succeeds, web traffic that is forwarded from the downstream proxy FortiGate to the upstream proxy can be accepted and forwarded to its destinations.

In this example, a school has a FortiGate acting as a downstream proxy that is configured with firewall policies for each user group: students, and staff. In each policy, a forwarding server is configured to forward the web traffic to the upstream web proxy.

The username and password that the upstream web proxy uses to authenticate the downstream proxy are configured on the forwarding server, and are sent to the upstream web proxy with the forwarded HTTP requests.

	Username	Password
student.proxy.local:8080	students	ABC123
staff.proxy.local:8081	staff	123456

On the downstream FortiGate, configure forwarding servers with the usernames and passwords for authentication on the upstream web proxy, then apply those servers to firewall policies for transparent proxy. For explicit web proxy, the forwarding servers can be applied to proxy policies.

When the transparent proxy is configured, clients can access websites without configuring a web proxy in their browser. The downstream proxy sends the username and password to the upstream proxy with forwarded HTTP requests to be authenticated.

#### To configure the forwarding server on the downstream FortiGate:

```
config web-proxy forward-server
  edit "Student_Upstream_WebProxy"
    set addr-type fqdn
    set fqdn "student.proxy.local"
    set port 8080
    set username "student"
    set password ABC123
  next
  edit "Staff_Upstream_WebProxy"
    set addr-type fqdn
    set fqdn "staff.proxy.local"
    set port 8081
    set username "staff"
    set password 123456
  next
end
```

#### To configure firewall policies for transparent proxy:

```
config firewall policy
  edit 1
    set srcintf "Vlan_Student"
    set dstintf "port9"
    set srcaddr "Student_Subnet"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set inspection-mode proxy
    set ssl-ssh-profile "deep-inspection"
    set av-profile "av"
    set webproxy-forward-server "Student_Upstream_WebProxy"
    set nat enable
  next
  edit 2
    set srcintf "Vlan_Staff"
    set dstintf "port9"
    set srcaddr "Staff_Subnet"
```



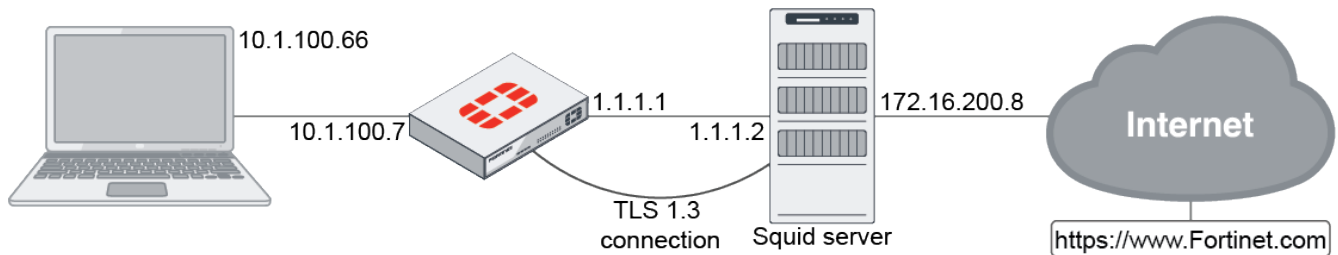
```
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set inspection-mode proxy
set ssl-ssh-profile "deep-inspection"
set av-profile "av"
set webproxy-forward-server "Staff_Upstream_WebProxy"
set nat enable
next
end
```

## Support TLS 1.3 for proxy forward servers in certificate inspection mode - 6.4.1

The FortiGate web proxy forward server now supports TLS 1.3. Prior to 6.4.1, if the server requested TLS 1.3, the web proxy forward configuration was unable to accommodate it, so no hello retry request was sent back to the client and the connection was stuck in the client hello phase.

### Example

In the following example, the Squid server and the FortiGate can handle TLS 1.3 traffic in both deep and certificate inspection modes.



The following output from the Squid server demonstrates that the FortiGate supports TLS 1.3 traffic and forwards the hello retry request back to the client PC. The client PC then sends the client hello again, and the connection is successfully established.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.100.66	13.56.33.144	TCP	72	58896 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=84354029 TSecr=0 s=128
2	0.000014	13.56.33.144	10.1.1.100.66	TCP	76	443 → 58896 [SYN, ACK] Seq=0 Ack=1 Win=16640 Len=0 MSS=1460 SACK_PERM=1 TSval=34678 TSecr=8435402
3	0.000141	10.1.1.100.66	13.56.33.144	TCP	66	58896 → 443 [ACK] Seq=1 Win=64256 Len=0 TSval=84354029 TSecr=34678
4	0.000275	10.1.1.100.66	13.56.33.144	TLSv1.3	583	Client Hello
5	0.000340	13.56.33.144	10.1.1.100.66	TCP	66	443 → 58896 [ACK] Seq=1 Ack=518 Win=15616 Len=0 TSval=34678 TSecr=84354025
6	0.000555	13.56.33.144	10.1.1.100.66	TLSv1.3	159	Hello Retry Request
7	0.000606	10.1.1.100.66	13.56.33.144	TCP	66	58896 → 443 [ACK] Seq=518 Ack=94 Win=64256 Len=0 TSval=84354079 TSecr=34682
8	0.000729	10.1.1.100.66	13.56.33.144	TLSv1.3	589	Change cipher spec, Client Hello
9	0.000852	13.56.33.144	10.1.1.100.66	TCP	66	443 → 58896 [ACK] Seq=94 Ack=1041 Win=16640 Len=0 TSval=34683 TSecr=84354080
10	0.077422	13.56.33.144	10.1.1.100.66	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
11	0.077437	13.56.33.144	10.1.1.100.66	TLSv1.3	1514	Application Data [CP segment of a reassembled PDU]
12	0.077640	13.56.33.144	10.1.1.100.66	TLSv1.3	317	Application Data, Application Data
13	0.078252	10.1.1.100.66	13.56.33.144	TCP	66	58896 → 443 [ACK] Seq=1041 Ack=3241 Win=62592 Len=0 TSval=84354108 TSecr=34685
14	0.079669	10.1.1.100.66	13.56.33.144	TLSv1.3	140	Application Data
15	0.081404	10.1.1.100.66	13.56.33.144	TLSv1.3	169	Application Data
16	0.081410	13.56.33.144	10.1.1.100.66	TCP	66	443 → 58896 [ACK] Seq=3241 Ack=1218 Win=16640 Len=0 TSval=34686 TSecr=84354109
17	0.101760	13.56.33.144	10.1.1.100.66	TLSv1.3	657	Application Data
18	0.101856	13.56.33.144	10.1.1.100.66	TLSv1.3	657	Application Data
19	0.102090	10.1.1.100.66	13.56.33.144	TCP	66	58896 → 443 [ACK] Seq=1218 Ack=4423 Win=64128 Len=0 TSval=84354131 TSecr=34688
20	0.112960	13.56.33.144	10.1.1.100.66	TLSv1.3	735	Application Data, Application Data, Application Data
21	0.115588	10.1.1.100.66	13.56.33.144	TLSv1.3	38	Application Data
22	0.116502	13.56.33.144	10.1.1.100.66	TCP	66	443 → 58896 [FIN, ACK] Seq=5092 Ack=1242 Win=16640 Len=0 TSval=34689 TSecr=84354145
23	0.116982	10.1.1.100.66	13.56.33.144	TCP	66	58896 → 443 [FIN, ACK] Seq=1242 Ack=5093 Win=64128 Len=0 TSval=84354145 TSecr=34689
24	0.116986	13.56.33.144	10.1.1.100.66	TCP	66	443 → 58896 [ACK] Seq=5093 Ack=1243 Win=16640 Len=0 TSval=34689 TSecr=84354145
						⚡
						⌵ Transmission Control Protocol, Src Port: 443, Dst Port: 58896, Seq: 1, Ack: 518, Len: 93
						⌵ Transport Layer Security
						⌵ TLSv1.3 Record Layer: Handshake Protocol: Hello Retry Request
						Content Type: Handshake (22)
						Version: TLS 1.2 (0x0303)
						Length: 88
						⌵ Handshake Protocol: Hello Retry Request
						Handshake Type: Server Hello (2)
						Length: 84
						Version: TLS 1.2 (0x0303)
						Random: c721a674e09a11b1b1b1b1b1b1b1b1b1c2a21167ab8b8c5w (HelloRetryRequest magic)
						Session ID Length: 32
						Session ID: 7d072100b019672bdc79b8e381c107273f3cd7a1b7f906w
						Cipher Suite: TLS_AES_128_GCM_SHA384 (0x1302)
						Compression Method: null (0)
						Extensions Length: 12
						⌵ Extension: supported_versions (len=2)
						Type: supported_versions (43)
						Length: 2
						Supported Versions: TLS 1.3 (0x0304)
						⌵ Extension: key_share (len=2)
						Type: key_share (51)
						Length: 2
						⌵ Key Share extension

# System

This section includes information about system related new features:

- [General on page 229](#)
- [High availability on page 236](#)
- [SNMP on page 249](#)
- [FortiGuard on page 255](#)

## General

This section includes information about general system related new features:

- [Admin profile option for diagnostic access on page 229](#)
- [FortinetOne renamed FortiCloud on page 230](#)
- [No session timeout on page 231](#)
- [Confirmation prompt when creating new VDOMs on page 232](#)
- [FortiOS image signing and verification on page 233](#)
- [Consistent style for replacement messages 6.4.2 on page 233](#)
- [Introduce maturity firmware levels 6.4.10 on page 235](#)
- [Enhance BIOS-level signature and file integrity checking 6.4.13 on page 236](#)

## Admin profile option for diagnostic access

The `system-diagnostics` command in an administrator profile can be used to control access to diagnose commands for global and VDOM level administrators.

### To block an administrator's access to diagnose commands:

1. Create an admin profile that cannot access diagnose commands:

```
config system accprofile
  edit "nodiagnose"
    ...
    set system-diagnostics disable
  next
end
```

2. Apply the profile to an administrator:

```
config system admin
  edit "nodiag"
    set accprofile "nodiagnose"
    set vdom "root"
    set password *****
```

```

    next
end

```

### 3. Log in as the administrator and confirm that they cannot access diagnose commands:

```

$ ?
config      Configure object.
get         Get dynamic and system information.
show        Show configuration.
execute     Execute static commands.
alias       Execute alias commands.
exit        Exit the CLI.

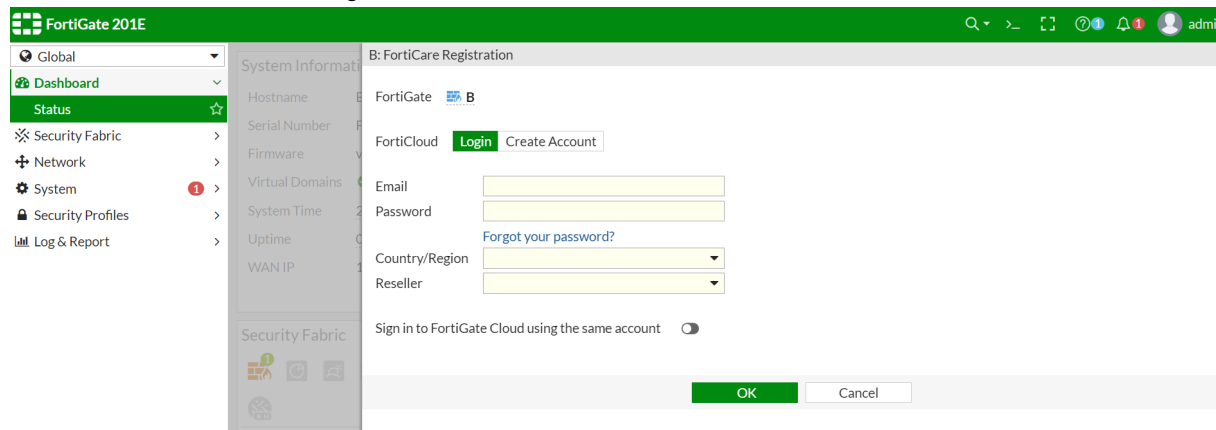
```

## FortinetOne renamed FortiCloud

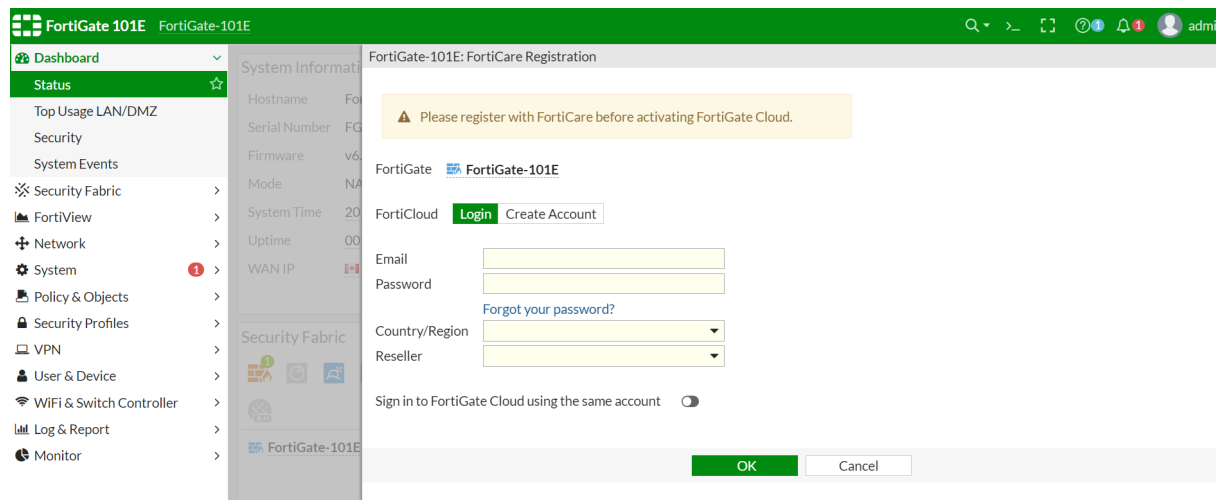
FortinetOne has been renamed FortiCloud in the FortiGate Cloud widget.

### To activate FortiGate Cloud and register with FortiCloud at the same time:

1. Go to *Dashboard > Status*.
2. In the *FortiGate Cloud* widget, click *Not Activated > Activate*.
3. In the *FortiCloud* area, click *Login*.



You must register with FortiCare before activating FortiCloud.



4. Enter your FortiCloud account credentials, and click *OK*.

## No session timeout

To allow clients to permanently connect with legacy medical applications and systems that do not have keepalive or auto-reconnect features, the session timeout can be set to never for firewall services, policies, and VDOMs.

The options to disable session timeout are hidden in the CLI.

### To set the session TTL value of a custom service to never:

```
config firewall service custom
  edit "tcp_23"
    set tcp-portrange 23
    set session-ttl never
  next
end
```

### To set the session TTL value of a policy to never:

```
config firewall policy
  edit 201
    set srcintf "wan1"
    set dstintf "wan2"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "TCP_8080"
    set logtraffic disable
    set session-ttl never
    set nat enable
  next
end
```

### To set the session TTL value of a VDOM to never:

```
config system session-ttl
  set default never
  config port
    edit 1
      set protocol 6
      set timeout never
      set start-port 8080
      set end-port 8080
    next
  end
end
```

### To view a session list with the timeout set to never:

```
# diagnose sys session list
```

```
session info: proto=6 proto_state=01 duration=9 expire=never timeout=never flags=00000000
```

```

sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty f00
statistic(bytes/packets/allow_err): org=2290/42/1 reply=2895/34/1 tuples=2
tx speed(Bps/kbps): 238/1 rx speed(Bps/kbps): 301/2
origin->sink: org pre->post, reply pre->post dev=18->17/17->18 gwy=172.16.200.55/10.1.100.41
hook=post dir=org act=snat 10.1.100.41:34256->172.16.200.55:23(172.16.200.10:34256)
hook=pre dir=reply act=dnat 172.16.200.55:23->172.16.200.10:34256(10.1.100.41:34256)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=9 auth_info=0 chk_client_info=0 vd=1
serial=00000b27 tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id = 00000000 ngfwid=n/a
dd_type=0 dd_mode=0
npu_state=0x000001 no_offload
no_ofld_reason: disabled-by-policy
total session 1

```

## Confirmation prompt when creating new VDOMs

A VDOM confirmation prompt has been added so users do not create new VDOMs accidentally in the CLI. This setting is disabled by default. Once enabled, when an administrator creates a new VDOM, the FortiGate displays a prompt to confirm before the VDOM is created.

### To use the VDOM confirmation prompt:

#### 1. Enable the prompt:

```

config system global
    set edit-vdom-prompt enable
end

```

#### 2. Create a new VDOM:

```

(global) # config vdom
    edit vdomtest1
    The input VDOM name doesn't exist.
    Do you want to create a new VDOM?
    Please press 'y' to continue, or press 'n' to cancel. (y/n)y

    current vf=vdomtest1:4

    next
    edit vdomtest2
    The input VDOM name doesn't exist.
    Do you want to create a new VDOM?
    Please press 'y' to continue, or press 'n' to cancel. (y/n)n

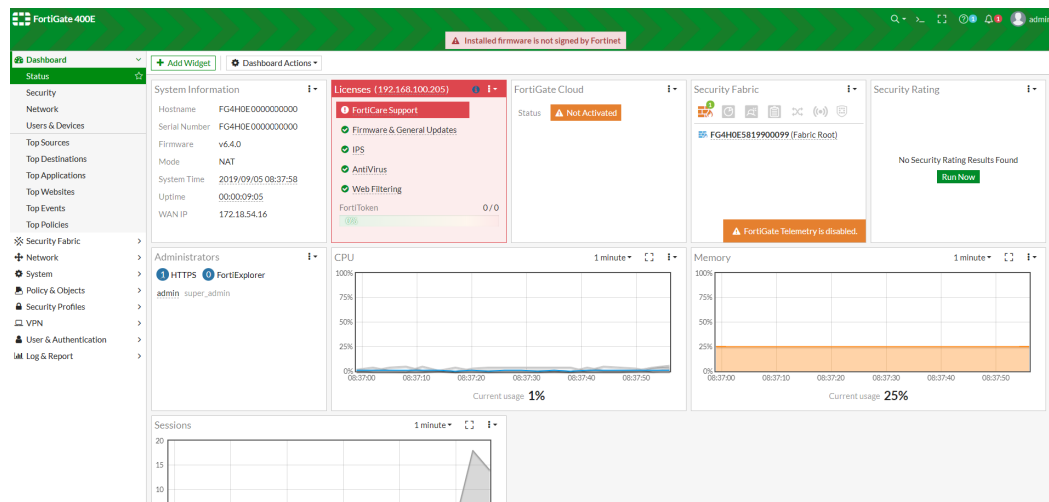
end

```

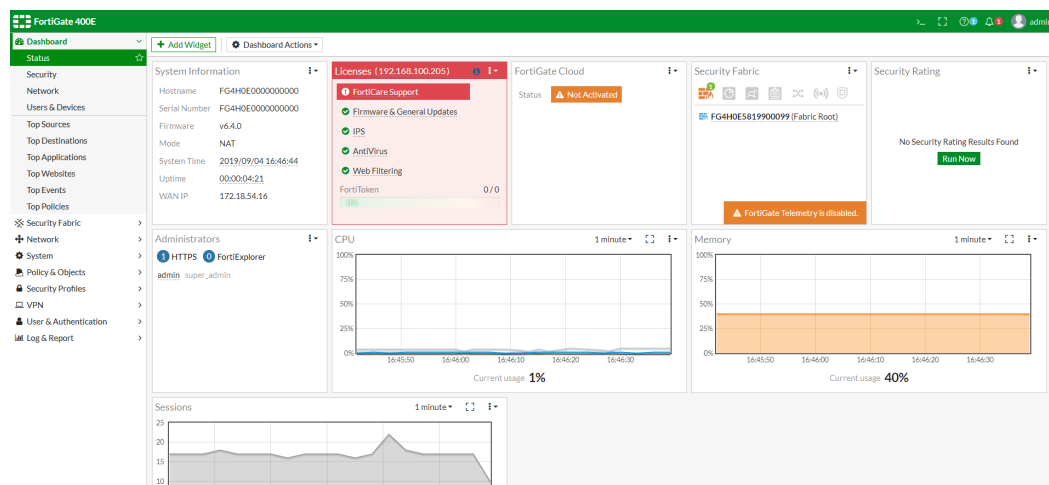
## FortiOS image signing and verification

Official FortiOS firmware images are signed by the Fortinet CA. The BIOS checks the validity of an image when it is uploaded to the device. If the image is not signed by the Fortinet CA, a warning message is shown in the GUI.

### Unsigned image:



### Signed image:



This feature is implemented on all FortiGate F-series models and E-series models released in 2019 and later.

## Consistent style for replacement messages - 6.4.2

The same style is used for the default HTML-based replacement messages. New replacement messages are added for UTM, and obsolete replacement messages are removed.

## Message examples

### Replacement message when traffic is blocked by the antivirus profile:



#### High Security Alert

You are not permitted to download the file "eicar" because it is infected with the virus "EICAR\_TEST\_FILE".

URL	<a href="http://172.16.200.55/virus/eicar">http://172.16.200.55/virus/eicar</a>
Quarantined File Name	
Reference URL	<a href="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE">http://www.fortinet.com/ve?vn=EICAR_TEST_FILE</a>
Username	
Group Name	

### Replacement message when traffic is blocked by the application control profile:



#### FortiGate Application Control

##### Application Blocked

You have attempted to use an application that violates your Internet usage policy.

Application	HTTP.BROWSER_Chrome
Category	Web.Client
URL	<a href="http://172.16.200.55/">http://172.16.200.55/</a>
Username	
Group Name	
Policy	c0e597c6-9eb6-51ea-33da-85f8db0bc680

## New messages

### To configure the new UTM replacement messages in the CLI:

```
config system replacemsg utm <msg-type>
```

Where `msg-type` can be:

- archive-block-html
- archive-block-text
- av-fail-text
- banned-word-html
- banned-word-text
- block-html
- block-text
- decompress-limit-text
- dlp-subject-text
- file-size-html



## Removed messages

The following replacement messages are removed:

Message category	Message type
<b>auth</b>	<ul style="list-style-type: none"> <li>auth-guest-print-page</li> </ul>
<b>fortiguard-wf</b>	<ul style="list-style-type: none"> <li>http-err</li> </ul>
<b>ftp</b>	<ul style="list-style-type: none"> <li>ftp-av-fail</li> <li>ftp-dl-archive-block</li> <li>ftp-dl-blocked</li> <li>ftp-dl-dlp-ban</li> <li>ftp-dl-filesize</li> <li>ftp-explicit-banner</li> <li>ftp-file-filter-block</li> </ul>
<b>http</b>	<ul style="list-style-type: none"> <li>bannedword</li> <li>http-archive-block</li> <li>http-block</li> <li>http-client-archive-block</li> <li>http-client-bannedword</li> <li>http-client-block</li> <li>http-client-filesize</li> <li>http-dlp-ban</li> <li>http-filesize</li> <li>http-post-block</li> </ul>
<b>mail</b>	<ul style="list-style-type: none"> <li>email-av-fail</li> <li>email-block</li> <li>email-decompress-limit</li> <li>email-dlp-ban</li> <li>email-dlp-subject</li> <li>email-file-filter</li> <li>email-filesize</li> <li>smtp-block</li> <li>smtp-decompress-limit</li> <li>smtp-filesize</li> </ul>
<b>spam</b>	<ul style="list-style-type: none"> <li>smtp-spam-bannedword</li> </ul>

## Introduce maturity firmware levels - 6.4.10

FortiOS 6.4.10 and later firmware images use tags to indicate the following maturity levels:

- The *Feature* tag indicates that the firmware release includes new features.
- The *Mature* tag indicates that the firmware release includes no new, major features. Mature firmware will contain bug fixes and vulnerability patches where applicable.

Administrators can use the `get system status` command to identify the maturity level of the current firmware.

For more information about this feature, see [Introduce maturity firmware levels](#).

## Enhance BIOS-level signature and file integrity checking - 6.4.13

The BIOS-level signature and file integrity checking has been enhanced for important system files and executables. Each release of AV and IPS engine files, FortiOS firmware and important executables are now dual signed by the Fortinet CA and a third-party CA. BIOS verifies each file matches their secure hash as indicated by their certificates. Users are warned when there is a failed integrity check, and the system may be prevented from booting depending on the severity and the BIOS security level.

Kernel and userspace processes can also periodically verify the integrity of the AV and IPS engine files, and other important system files and executables. They can also cease the FortiGate from operating when the monitored files fail to match their secure hashes.

In summary, the enhanced BIOS-level signature and file integrity check allows the FortiGate to identify tampering of important system and executable files, warn users of the breaches, and prevent malicious code from running on the system.

For more information about this feature, see [Enhance BIOS-level signature and file integrity checking](#).

## High availability

This section includes information about HA related new features:

- [Force HA failover for testing and demonstrations on page 236](#)
- [Support UTM inspection on asymmetric traffic in FGSP on page 239](#)
- [Support UTM inspection on asymmetric traffic on L3 on page 241](#)
- [Add encryption for L3 on asymmetric traffic in FGSP on page 243](#)
- [Override FortiAnalyzer and syslog server settings on page 243](#)
- [Source interface setting for NetFlow data on page 247](#)
- [Applying the session synchronization filter only between FGSP peers in an FGCP over FGSP topology 6.4.10 on page 249](#)

### Force HA failover for testing and demonstrations



This command should only be used for testing, troubleshooting, maintenance, and demonstrations.

Do not use it in a live production environment outside of an active maintenance window.

---

HA failover can be forced on an HA primary device. The device will stay in a failover state regardless of the conditions. The only way to remove the failover status is by manually turning it off.

#### Syntax

```
execute ha failover set <cluster_id>
execute ha failover unset <cluster_id>
```

Variable	Description
<cluster_id>	The cluster ID is 1 for any cluster that is not in virtual cluster mode, and can be 1 or 2 if virtual cluster mode is enabled.

## Example

### To manually force an HA failover:

```
# execute ha failover set 1
Caution: This command will trigger an HA failover.
It is intended for testing purposes.
Do you want to continue? (y/n)y
```

### To view the failover status:

```
# execute ha failover status
failover status: set
```

### To view the system status of a device in forced HA failover:

```
# get system ha status
HA Health Status: OK
Model: FortiGate-300D
Mode: HA A-P
Group: 240
Debug: 0
Cluster Uptime: 0 days 2:11:46
Cluster state change time: 2020-03-12 17:38:04
Master selected using:
    <2020/03/12 17:38:04> FGT3HD3914800153 is selected as the master because it has EXE_
    FAIL_OVER flag set.
    <2020/03/12 15:27:26> FGT3HD3914800069 is selected as the master because it has the
    largest value of override priority.
ses_pickup: disable
override: enable
Configuration Status:
    FGT3HD3914800069(updated 4 seconds ago): in-sync
    FGT3HD3914800153(updated 3 seconds ago): in-sync
System Usage stats:
    FGT3HD3914800069(updated 4 seconds ago):
        sessions=5, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=30%
    FGT3HD3914800153(updated 3 seconds ago):
        sessions=41, average-cpu-user/nice/system/idle=0%/0%/0%/99%, memory=30%
HBDEV stats:
    FGT3HD3914800069(updated 4 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=15914162/42929/0/0,
        tx=15681840/39505/0/0
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=17670346/52854/0/0,
        tx=20198409/54692/0/0
    FGT3HD3914800153(updated 3 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=16636700/45544/0/0,
        tx=15529791/39512/0/0
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=20199928/54699/0/0,
```

```

tx=17672146/52862/0/0
Slave : FortiGate-300D , FGT3HD3914800069, HA cluster index = 1
Master: FortiGate-300D , FGT3HD3914800153, HA cluster index = 0
number of vcluster: 1
vcluster 1: standby 169.254.0.1
Slave : FGT3HD3914800069, HA operating index = 1
Master: FGT3HD3914800153, HA operating index = 0

```

### To stop the failover status:

```

# execute ha failover unset 1
Caution: This command may trigger an HA failover.
It is intended for testing purposes.
Do you want to continue? (y/n)y

```

### To view the system status of a device after forced HA failover is disabled:

```

# get system ha status
HA Health Status: OK
Model: FortiGate-300D
Mode: HA A-P
Group: 240
Debug: 0
Cluster Uptime: 0 days 2:14:55
Cluster state change time: 2020-03-12 17:42:17
Master selected using:
    <2020/03/12 17:42:17> FGT3HD3914800069 is selected as the master because it has the
largest value of override priority.
    <2020/03/12 17:38:04> FGT3HD3914800153 is selected as the master because it has EXE_
FAIL_OVER flag set.
    <2020/03/12 15:27:26> FGT3HD3914800069 is selected as the master because it has the
largest value of override priority.
ses_pickup: disable
override: enable
Configuration Status:
    FGT3HD3914800069(updated 3 seconds ago): in-sync
    FGT3HD3914800153(updated 2 seconds ago): in-sync
System Usage stats:
    FGT3HD3914800069(updated 3 seconds ago):
        sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=30%
    FGT3HD3914800153(updated 2 seconds ago):
        sessions=38, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=30%
HBDEV stats:
    FGT3HD3914800069(updated 3 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=16302442/43964/0/0,
tx=16053848/40454/0/0
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=18161941/54088/0/0,
tx=20615650/55877/0/0
    FGT3HD3914800153(updated 2 seconds ago):
        port3: physical/1000auto, up, rx-bytes/packets/dropped/errors=17033009/46641/0/0,
tx=15907891/40462/0/0
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=20617180/55881/0/0,
tx=18163135/54091/0/0
Master: FortiGate-300D , FGT3HD3914800069, HA cluster index = 1
Slave : FortiGate-300D , FGT3HD3914800153, HA cluster index = 0
number of vcluster: 1

```

```
vcluster 1: work 169.254.0.2
Master: FGT3HD3914800069, HA operating index = 0
Slave : FGT3HD3914800153, HA operating index = 1
```

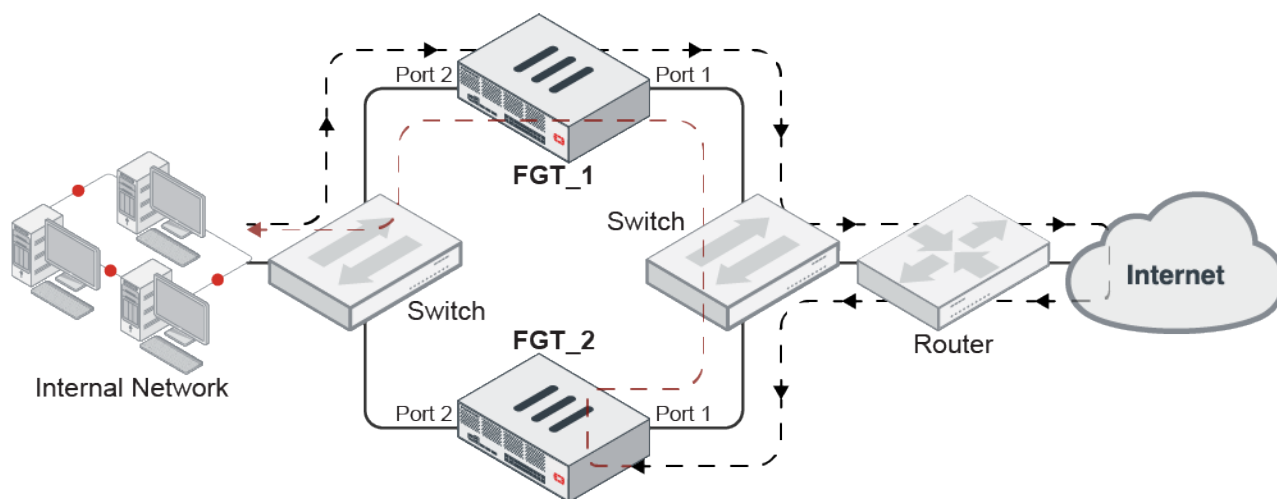
## Support UTM inspection on asymmetric traffic in FGSP

When traffic passes asymmetrically through FGSP peers, UTM inspection can be supported by always forwarding traffic back to the session owner for processing. The session owner is the FortiGate that receives the first packet of the session.

In this example, traffic from the internal network first hits FGT\_1, but the return traffic is routed to FGT\_2. Consequently, traffic bounces from FGT\_2 port1 to FGT\_1 port1 using FGT\_1's MAC address. Traffic is then inspected by FGT\_1.

This example requires the following settings:

- Internal and outgoing interfaces of both FortiGates in the FGSP pair are in the same subnet.
- Both peers have layer 2 access with each other.



### To configure FTG\_1:

1. Configure the cluster, setting the peer IP to the IP address of FGT\_2:

```
config system cluster-sync
  edit 1
    set peerip 10.2.2.2
  next
end
```

2. Configure FGSP cluster attributes:

```
config system standalone-cluster
  set standalone-group-id 1
  set group-member-id 0
  set layer2-connection available
  unset session-sync-dev
end
```

### 3. Configure the firewall policy:

```
config firewall policy
  edit 1
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set av-profile "default"
    set logtraffic all
    set nat enable
  next
end
```

### To configure FTG\_2:

#### 1. Configure the cluster, setting the peer IP to the IP address of FGT\_1:

```
config system cluster-sync
  edit 1
    set peerip 10.2.2.1
  next
end
```

#### 2. Configure FGSP cluster attributes:

```
config system standalone-cluster
  set standalone-group-id 1
  set group-member-id 1
  set layer2-connection available
  unset session-sync-dev
end
```

#### 3. Configure the firewall policy:

```
config firewall policy
  edit 1
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set av-profile "default"
    set logtraffic all
    set nat enable
  next
end
```

## Results

Capture packets on FGT\_2 to see that traffic bounced from FGT\_2 to FGT\_1 over the traffic interface.

```

FGT_2 # diagnose sniffer packet any 'host 10.1.100.15 and host 172.6.200.55' 4
interfaces=[any]
filters=[host 10.1.100.15 and host 172.16.200.55]
91.803816 port1 in 172.16.200.55.80 -> 10.1.100.15.40008: syn 2572073713 ack 261949279
92.800480 port1 in 172.16.200.55.80 -> 10.1.100.15.40008: syn 2572073713 ack 261949279
92.800486 port1 out 172.16.200.55.80 -> 10.1.100.15.40008: syn 2572073713 ack 261949279
92.800816 port1 in 172.16.200.55.80 -> 10.1.100.15.40008: syn 2572073713 ack 261949279
92.800818 port1 out 172.16.200.55.80 -> 10.1.100.15.40008: syn 2572073713 ack 261949279

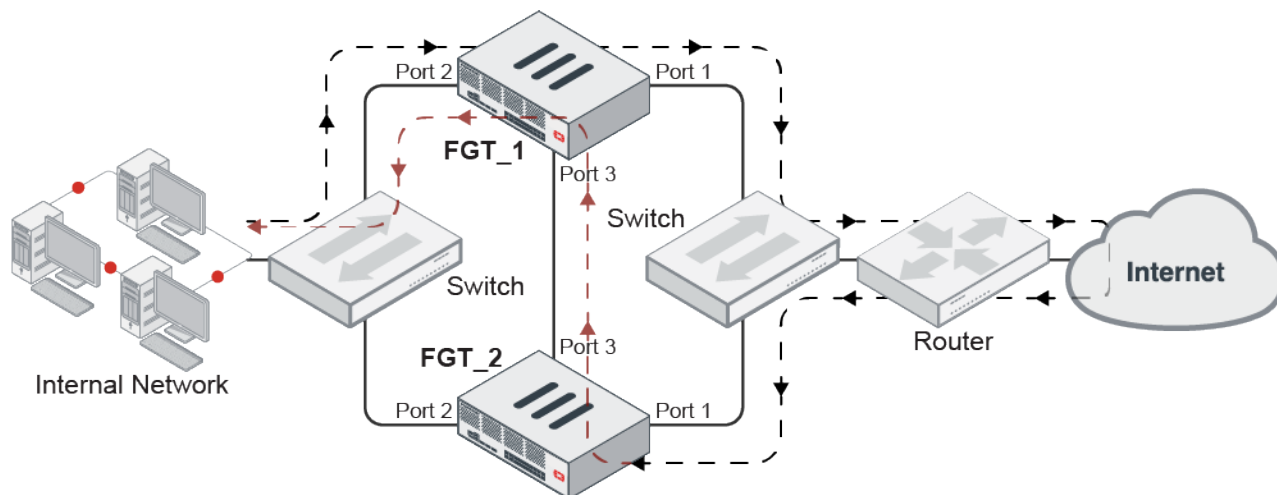
```

## Support UTM inspection on asymmetric traffic on L3

When traffic passes asymmetrically through FGSP peers, UTM inspection can be supported by always forwarding traffic back to the session owner for processing. The session owner is the FortiGate that receives the first packet of the session.

For networks where L2 connectivity is not available, such as cloud environments, traffic bound for the session owner are forwarded through the peer interface using a UDP connection.

In this example, traffic from the internal network first hits FGT\_1, but the return traffic is routed to FGT\_2. Consequently, return traffic is packed and sent from FGT\_2 to FGT\_1 using UDP encapsulation between two peer interfaces (port 3). Traffic is then inspected by FGT\_1.



### To configure FTG\_1:

1. Configure the cluster, setting the peer IP to the IP address of FGT\_2:

```

config system cluster-sync
  edit 1
    set peerip 10.2.2.2
  next
end

```

2. Configure FGSP cluster attributes:

```

config system standalone-cluster
  set standalone-group-id 1
  set group-member-id 0
  set layer2-connection unavailable

```

```
    unset session-sync-dev
end
```

### 3. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set av-profile "default"
        set logtraffic all
        set nat enable
    next
end
```

## To configure FTG\_2:

### 1. Configure the cluster, setting the peer IP to the IP address of FGT\_1:

```
config system cluster-sync
    edit 1
        set peerip 10.2.2.1
    next
end
```

### 2. Configure FGSP cluster attributes:

```
config system standalone-cluster
    set standalone-group-id 1
    set group-member-id 1
    set layer2-connection unavailable
    unset session-sync-dev
end
```

### 3. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set av-profile "default"
        set logtraffic all
        set nat enable
    next
end
```



## Add encryption for L3 on asymmetric traffic in FGSP

In scenarios where asymmetric routing between FGSP members occurs, the return traffic can be routed back to the session owner in Layer 3 (L3). This L3 traffic can now be encrypted.

### To encrypt L3 traffic in FGSP:

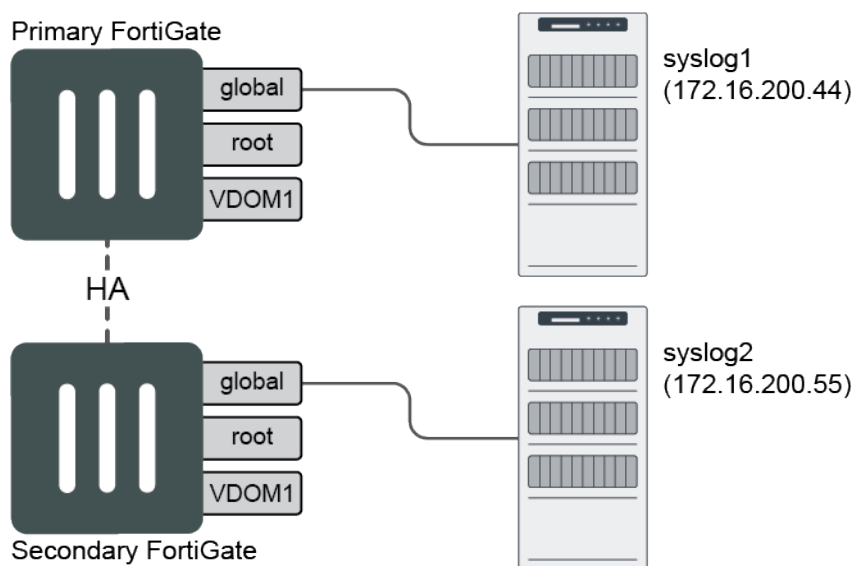
1. Run the following on both FortiGates:

```
config system standalone-cluster
    set encryption enable
    set psksecret xxxxxxxxxx
end
```

## Override FortiAnalyzer and syslog server settings

In an HA cluster, secondary devices can be configured to use different FortiAnalyzer devices and syslog servers than the primary device. VDOMs can also override global syslog server settings.

### Configure a different syslog server on a secondary HA device



### To configure the primary HA device:

1. Configure a global syslog server:

```
config global
    config log syslog setting
        set status enable
        set server 172.16.200.44
        set facility local6
        set format default
```

```

end
end

```

## 2. Set up a VDOM exception to enable setting the global syslog server on the secondary HA device:

```

config global
    config system vdom-exception
        edit 1
            set object log.syslogd.setting
        next
    end
end

```

## To configure the secondary HA device:

### 1. Configure a global syslog server:

```

config global
    config log syslogd setting
        set status enable
        set server 172.16.200.55
        set facility local5
    end
end

```

### 2. After the primary and secondary device synchronize, generate logs on the secondary device.

## To confirm that logs are been sent to the syslog server configured on the secondary device:

### 1. On the primary device, retrieve the following packet capture from the secondary device's syslog server:

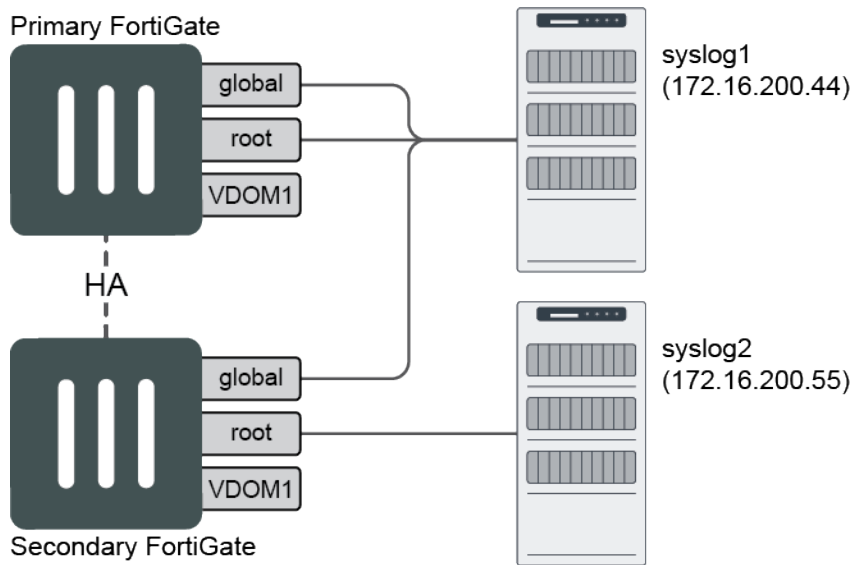
```

# diagnose sniffer packet any "host 172.16.200.55" 6
interfaces=[any]
filters=[host 172.16.200.55]

266.859494 port2 out 172.16.200.2.7434 -> 172.16.200.55.514: udp 278
0x0000  0000 0000 0000 0009 0f09 0004 0800 4500      .....E.
0x0010  0132 f3c7 0000 4011 9d98 ac10 c802 ac10      .2....@.....
0x0020  c837 1d0a 0202 011e 4b05 3c31 3734 3e64      .7.....K.<174>d
0x0030  6174 653d 3230 3230 2d30 332d 3134 2074      ate=2020-03-14.t
0x0040  696d 653d 3132 3a30 303a 3035 2064 6576      ime=12:00:05.dev
0x0050  6e61 6d65 3d22 466f 7274 6947 6174 652d      name="FGT-81E-Sl
0x0060  3831 455f 4122 2064 6576 6964 3d22 4647      ave-A".devid="FG
0x0070  5438 3145 3451 3136 3030 3030 3438 2220      T81E4Q16000048".
0x0080  6c6f 6769 643d 2230 3130 3030 3230 3032      logid="010002002
0x0090  3722 2074 7970 653d 2265 7665 6e74 2220      7".type="event".
0x00a0  7375 6274 7970 653d 2273 7973 7465 6d22      subtype="system"
0x00b0  206c 6576 656c 3d22 696e 666f 726d 6174      .level="informat
0x00c0  696f 6e22 2076 643d 2276 646f 6d31 2220      ion".vd="vdom1".
0x00d0  6576 656e 7474 696d 653d 3135 3834 3231      eventtime=158421
0x00e0  3234 3035 3835 3938 3335 3639 3120 747a      2405859835691.tz
0x00f0  3d22 2d30 3730 3022 206c 6f67 6465 7363      ="-0700".logdesc
0x0100  3d22 4f75 7464 6174 6564 2072 6570 6f72      ="Outdated.repor
0x0110  7420 6669 6c65 7320 6465 6c65 7465 6422      t.files.deleted"
0x0120  206d 7367 3d22 4465 6c65 7465 2031 206f      .msg="Delete.1.o
0x0130  6c64 2072 6570 6f72 7420 6669 6c65 7322      ld.report.files"

```

## Configure a different syslog server in the root VDOM on a secondary HA device



### To configure the primary HA device:

#### 1. Configure a global syslog server:

```
config global
    config log syslog setting
        set status enable
        set server 172.16.200.44
        set facility local6
        set format default
    end
end
```

#### 2. Set up a VDOM exception to enable syslog-override in the secondary HA device root VDOM:

```
config global
    config system vdom-exception
        edit 1
            set object log.syslogd.override-setting
            set scope inclusive
            set vdom root
        next
    end
end
```

#### 3. In the VDOM, enable syslog-override in the log settings, and set up the override syslog server:

```
config root
    config log setting
        set syslog-override enable
    end
    config log syslog override-setting
        set status enable
        set server 172.16.200.44
        set facility local6
    end
end
```

```

        set format default
    end
end

```

After `syslog-override` is enabled, an override syslog server must be configured, as logs will not be sent to the global syslog server.

### To configure the secondary HA device:

1. Configure an override syslog server in the root VDOM:

```

config root
    config log syslogd override-setting
        set status enable
        set server 172.16.200.55
        set facility local5
        set format default
    end
end

```

2. After the primary and secondary device synchronize, generate logs in the root VDOM on the secondary device.

### To confirm that logs are been sent to the syslog server configured for the root VDOM on the secondary device:

1. On the primary device, retrieve the following packet capture from the syslog server configured in the root VDOM on the secondary device:

```

# diagnose sniffer packet any "host 172.16.200.55" 6
interfaces=[any]
filters=[host 172.16.200.55]

156.759696 port2 out 172.16.200.2.1165 -> 172.16.200.55.514: udp 277
0x0000  0000 0000 0000 0009 0f09 0004 0800 4500      .....E.
0x0010  0131 f398 0000 4011 9dc8 ac10 c802 ac10      .1....@.....
0x0020  c837 048d 0202 011d af5f 3c31 3734 3e64      .7....._<174>d
0x0030  6174 653d 3230 3230 2d30 332d 3134 2074      ate=2020-03-14.t
0x0040  696d 653d 3131 3a33 353a 3035 2064 6576      ime=11:35:05.dev
0x0050  6e61 6d65 3d22 466f 7274 6947 6174 652d      name="FGT-81E-Sl
0x0060  3831 455f 4122 2064 6576 6964 3d22 4647      ave-A".devide="FG
0x0070  5438 3145 3451 3136 3030 3030 3438 2220      T81E4Q16000048".
0x0080  6c6f 6769 643d 2230 3130 3030 3230 3032      logid="010002002
0x0090  3722 2074 7970 653d 2265 7665 6e74 2220      7".type="event".
0x00a0  7375 6274 7970 653d 2273 7973 7465 6d22      subtype="system"
0x00b0  206c 6576 656c 3d22 696e 666f 726d 6174      .level="informat
0x00c0  696f 6e22 2076 643d 2272 6f6f 7422 2065      ion".vd="root".e
0x00d0  7665 6e74 7469 6d65 3d31 3538 3432 3130      venttime=1584210
0x00e0  3930 3537 3539 3334 3132 3632 2074 7a3d      905759341262.tz=
0x00f0  222d 3037 3030 2220 6c6f 6764 6573 633d      "-0700".logdesc=
0x0100  224f 7574 6461 7465 6420 7265 706f 7274      "Outdated.report
0x0110  2066 696c 6573 2064 656c 6574 6564 2220      .files.deleted".
0x0120  6d73 673d 2244 656c 6574 6520 3220 6f6c      msg="Delete.2.ol
0x0130  6420 7265 706f 7274 2066 696c 6573 22      d.report.files"

```

## Source interface setting for NetFlow data

NetFlow data can be routed over the HA management interface when the `ha-direct` option is enabled. The secondary unit does not send out any flow data whether it is running in A-A or A-P.

### To route NetFlow data over the HA management interface:

1. On the primary unit (FortiGate A), configure the HA and mgmt1 interface settings:

```
(global) # config system ha
    set group-name "test-ha"
    set mode a-p
    set password ENC
    set hbdev "port6" 50
    set hb-interval 4
    set hb-lost-threshold 10
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "mgmt1"
        next
    end
    set override enable
    set priority 200
    set ha-direct enable
end

(global) # config system interface
    edit "mgmt1"
        set ip 10.6.30.111 255.255.255.0
        set allowaccess ping https ssh http telnet fgfm
        set type physical
        set dedicated-to management
        set role lan
        set snmp-index 1
    next
end
```

2. On the secondary unit (FortiGate B), configure the HA and mgmt1 interface settings:

```
(global) # config system ha
    set group-name "test-ha"
    set mode a-p
    set password ENC
    set hbdev "port6" 50
    set hb-interval 4
    set hb-lost-threshold 10
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "mgmt1"
        next
    end
    set override enable
```

```

        set priority 100
        set ha-direct enable
    end

(global) # config system interface
    edit "mgmt1"
        set ip 10.6.30.112 255.255.255.0
        set allowaccess ping https ssh http telnet fgfm
        set type physical
        set dedicated-to management
        set role lan
        set snmp-index 1
    next
end

```

**3. On the primary unit (FortiGate A), configure the NetFlow setting:**

```

(global) # config system netflow
    set collector-ip 10.6.30.59
end

```

When the `ha-direct` option is enabled in `config system ha`, FortiOS is no longer allowed to set `source-ip` in `config system netflow`.

**4. Verify that NetFlow uses the mgmt1 IP:**

```

(global) # diagnose test application sflowd 3

```

**5. Verify that the NetFlow packets are being sent by the mgmt1 IP:**

```

(vdom1) # diagnose sniffer packet any 'udp and port 2055' 4
interfaces=[any]
filters=[udp and port 2055]
8.397265 mgmt1 out 10.6.30.111.1992 -> 10.6.30.59.2055: udp 60
23.392175 mgmt1 out 10.6.30.111.1992 -> 10.6.30.59.2055: udp 188
23.392189 mgmt1 out 10.6.30.111.1992 -> 10.6.30.59.2055: udp 60
^C
3 packets received by filter
0 packets dropped by kernel

```

**6. On the secondary device (FortiGate B), change the priority so that it becomes the primary:**

```

(global) # config system ha
    set priority 250
end

```

**7. Verify the NetFlow status on FortiGate A, which is using the new primary unit's mgmt1 IP:**

```

(global) # diagnose test application sflowd 3

```

**8. Verify that the NetFlow packets use the new source IP on FortiGate B:**

```

(vdom1) # diagnose sniffer packet any 'udp and port 2055' 4
interfaces=[any]
filters=[udp and port 2055]
7.579574 mgmt1 out 10.6.30.112.3579 -> 10.6.30.59.2055: udp 60
22.581830 mgmt1 out 10.6.30.112.3579 -> 10.6.30.59.2055: udp 60
29.038336 mgmt1 out 10.6.30.112.3579 -> 10.6.30.59.2055: udp 1140
^C
3 packets received by filter
0 packets dropped by kernel

```

## Applying the session synchronization filter only between FGSP peers in an FGCP over FGSP topology - 6.4.10

This enhancement ensures that session synchronization happens correctly in an FGCP over FGSP topology:

- When the session synchronization filter is applied on FGSP, the filter will only affect sessions synchronized between the FGSP peers.
- When virtual clustering is used, sessions synchronized between each virtual cluster can also be synchronized to FGSP peers. All peers' `syncvd` must be in the same HA virtual cluster.

For more information about this feature, see [Applying the session synchronization filter only between FGSP peers in an FGCP over FGSP topology](#).



This topic uses `config system standalone-cluster` to configure the FGSP peers. In FortiOS 6.4, the peers are configured using `config system standalone-cluster` and `config system cluster-sync`.

## SNMP

This section includes information about SNMP related new features:

- [SNMP bridge MIB module support on page 249](#)
- [Support SHA-2 for SNMPv3 on page 251](#)
- [SNMP traps and query for monitoring DHCP pool on page 252](#)
- [SNMP polling extensions to support new OIDs 6.4.2 on page 253](#)
- [SNMP OIDs for port block allocations IP pool statistics 6.4.12 on page 255](#)

### SNMP bridge MIB module support



This feature is only available on FortiGate Rugged 30D, which supports 802.1p.

SNMP bridge MIB module support is available on FortiGates with 802.1p to monitor STP activity.

The following OIDs have been added:

Object name	OID
dot1dBridge.dot1dBase.dot1dBaseBridgeAddress	1.3.6.1.2.1.17.1.1
dot1dBridge.dot1dBase.dot1dBaseNumPorts	1.3.6.1.2.1.17.1.2
dot1dBridge.dot1dBase.Type	1.3.6.1.2.1.17.1.3
dot1dBridge.dot1dBase.dot1dBasePortEntry.dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

Object name	OID
dot1dBridge.dot1dBase.dot1dBasePortEntry.dot1dBasePortCircuit	1.3.6.1.2.1.17.1.4.1.3
dot1dBridge.dot1dBase.dot1dBasePortEntry.dot1dBasePortDelayExceededDiscards	1.3.6.1.2.1.17.1.4.1.5
dot1dBridge.dot1dBase.dot1dBasePortEntry.dot1dBasePortMtuExceededDiscards	1.3.6.1.2.1.17.1.4.1.5
dot1dBridge.dot1dStp.dot1dStpProtocolSpecification	1.3.6.1.2.1.17.2.1
dot1dBridge.dot1dStp.dot1dStpPriority	1.3.6.1.2.1.17.2.2
dot1dBridge.dot1dStp.dot1dStpDesignatedRoot	1.3.6.1.2.1.17.2.5
dot1dBridge.dot1dStp.dot1dStpRootCost	1.3.6.1.2.1.17.2.6
dot1dBridge.dot1dStp.dot1dStpRootPort	1.3.6.1.2.1.17.2.7
dot1dBridge.dot1dStp.dot1dStpMaxAge	1.3.6.1.2.1.17.2.8
dot1dBridge.dot1dStp.dot1dStpHelloTime	1.3.6.1.2.1.17.2.9
dot1dBridge.dot1dStp.dot1dStpForwardDelay	1.3.6.1.2.1.17.2.11
dot1dBridge.dot1dStp.dot1dStpBridgeMaxAge	1.3.6.1.2.1.17.2.12
dot1dBridge.dot1dStp.dot1dStpBridgeHelloTime	1.3.6.1.2.1.17.2.13
dot1dBridge.dot1dStp.dot1dStpBridgeForwardDelay	1.3.6.1.2.1.17.2.14
dot1dBridge.dot1dStp.dot1dStpPortEntry.dot1dStpPortPriority	1.3.6.1.2.1.17.2.15.1.2
dot1dBridge.dot1dStp.dot1dStpPortEntry.dot1dStpPortState	1.3.6.1.2.1.17.2.15.1.3
dot1dBridge.dot1dStp.dot1dStpPortEntry.dot1dStpPortEnable	1.3.6.1.2.1.17.2.15.1.4
dot1dBridge.dot1dStp.dot1dStpPortEntry.dot1dStpPortPathCost	1.3.6.1.2.1.17.2.15.1.5

### To configure an SNMP bridge MIB module:

#### 1. On the FortiGate, configure SNMP:

```

config system snmp sysinfo
    set status enable
    set description "BRIDGE_MIB"
    set contact-info "Strike Freedom"
    set location "QA LAB"
end

config system snmp community
    edit 1
        set name "REGR-SWITCH"
        config hosts
            edit 1
                set ip 172.16.200.55 255.255.255.255
            next
            edit 2
                set ip 172.18.60.149 255.255.255.255
            next
        end
        set events cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch
    
```



```

ha-hb-failure ips-anomaly av-oversize av-fragmented fm-conf-change ha-member-up ha-
member-down av-conserve av-bypass av-oversize-blocked ips-pkg-update ips-fail-open faz-
disconnect
    next
end

```

2. On the SNMP server, run `snmpwalk` on the OID from the newly added bridge MIB.

The OID is for the bridge hello time. The SNMP server is able to query the bridge hello time from the FortiGate:

```

root@ControlPC:~# snmpwalk -v1 -c REGR-SWITCH 172.16.200.2 1.3.6.1.2.1.17.2.13
BRIDGE-MIB::dot1dStpBridgeHelloTime.0 = INTEGER: 200 centi-seconds

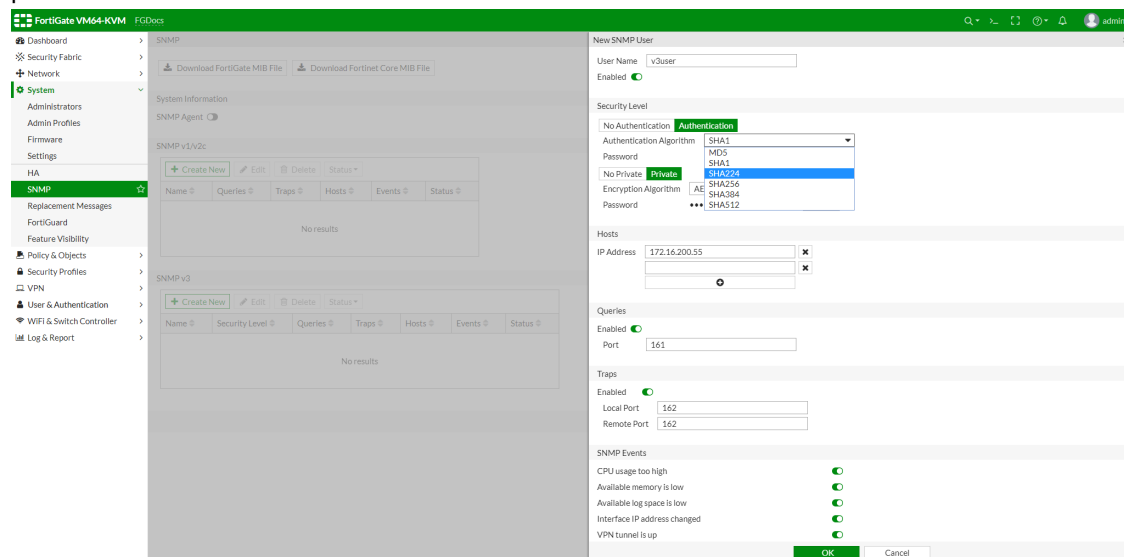
```

## Support SHA-2 for SNMPv3

SNMPv3 supports HMAC-SHA-2 authentication protocols based on the following SHA-2 hash functions: SHA-224, SHA-256, SHA-384, and SHA-512.

### To configure an SNMPv3 user in the GUI:

1. Go to *System > SNMP*.
2. In the *SNMPv3* section, click *Create New*. The *New SNMP User* pane opens.
3. In the *Security Level* section, click *Authentication* and for *Authentication Algorithm*, select a SHA-2 authentication protocol.



4. Configure the other settings as needed.
5. Click **OK**.

### To configure an SNMPv3 user in the CLI:

```

config system snmp user
    edit "v3user"
        set security-level auth-priv
        set auth-proto {md5 | sha | sha224 | sha256 | sha384 | sha512}
        set auth-pwd xxxxxxxx
        set priv-pwd xxxxxxxx
    end
end

```

```

next
end

```

## SNMP traps and query for monitoring DHCP pool

The SNMP DHCP event contains three traps and one query.

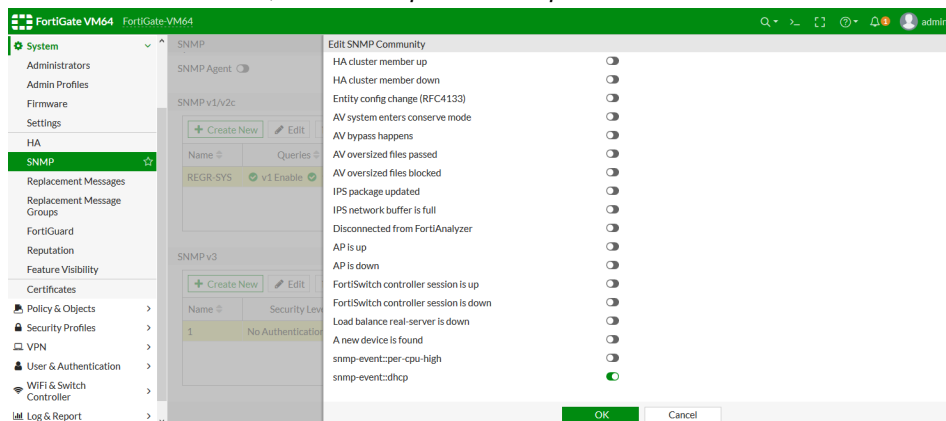
Traps are sent when:

- DHCP server IP pool usage reaches 90%
- DHCP server detect an IP address that is already in use
- DHCP client receives DHCP NAK

SNMP queries are accepted for DHCP lease usage information (OID = 1.3.6.1.4.1.12356.101.23). The query result is based on the leased out percentage.

**To enable the SNMP DHCP event in the GUI:**

1. Go to *System > SNMP*.
2. Click *Create New* in either the *SNMP v1/v2c* table or *SNMP v3* table, or edit an existing community or user.
3. Configure the settings as required.
4. In the *SNMP Events* list, enable *snmp-event::dhcp*.



5. Click **OK**.

**To enable the SNMP DHCP event in the CLI:**

```

config system snmp community
edit 1
set name "REGR-SYS"
config hosts
edit 1
set ip 10.1.100.11 255.255.255.255
next
edit 2
set ip 172.16.200.55 255.255.255.255
next
end
set events dhcp

```

```
    next
end
config system snmp user
    edit "1"
        set notify-hosts 172.10.1.0 172.20.1.0
        set events dhcp
        set security-level auth-priv
        set auth-proto sha384
        set auth-pwd *****
        set priv-proto aes256
        set priv-pwd *****
    next
end
```

## SNMP polling extensions to support new OIDs - 6.4.2

New OIDs are added to support SNMP query for license details and IPsec tunnels.

### To configure SNMP:

```
config system snmp community
    edit 1
        set name "SNMP-TEST"
        config hosts
            edit 1
                set ip 10.1.100.11 255.255.255.255
            next
            edit 2
                set ip 172.16.200.55 255.255.255.255
            next
        end
        config hosts6
            edit 1
                set ipv6 2000:172:16:200::55/128
            next
            edit 2
                set ipv6 2000:10:1:100::11/128
            next
        end
        set events cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch ha-
hb-failure ips-signature ips-anomaly av-virus av-oversize av-pattern av-fragmented fm-if-
change fm-conf-change ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-
oversize-passed av-oversize-blocked ips-pkg-update faz-disconnect
    next
end
```

### License details

New OIDs are added in *fgSystemInfoAdvanced* to support SNMP query for license details, including the following two tables.

**fgLicContracts 1.3.6.1.4.1.12356.101.4.6.3.1**

```
snmpwalk -v2c -c SNMP-TEST 172.16.200.1 1.3.6.1.4.1.12356.101.4.6.3.1
```

```

FORTINET-FORTIGATE-MIB::fgLicContractCount.0 = INTEGER: 28
FORTINET-FORTIGATE-MIB::fgLicContractDesc.1 = STRING: Hardware
FORTINET-FORTIGATE-MIB::fgLicContractDesc.2 = STRING: Enhanced
FORTINET-FORTIGATE-MIB::fgLicContractDesc.3 = STRING: Firmware & general updates
FORTINET-FORTIGATE-MIB::fgLicContractDesc.4 = STRING: FortiClient
FORTINET-FORTIGATE-MIB::fgLicContractDesc.5 = STRING: Webfilter
FORTINET-FORTIGATE-MIB::fgLicContractDesc.6 = STRING: Virus Definitions
FORTINET-FORTIGATE-MIB::fgLicContractDesc.7 = STRING: Security Rating license
FORTINET-FORTIGATE-MIB::fgLicContractDesc.8 = STRING: SPRT
...

```

#### **fgLicVersions 1.3.6.1.4.1.12356.101.4.6.3.2**

```

snmpwalk -v2c -c SNMP-TEST 172.16.200.1 1.3.6.1.4.1.12356.101.4.6.3.2 (Version info)
FORTINET-FORTIGATE-MIB::fgLicVersionCount.0 = INTEGER: 25
FORTINET-FORTIGATE-MIB::fgLicVersionDesc.1 = STRING: Application Definitions
FORTINET-FORTIGATE-MIB::fgLicVersionDesc.2 = STRING: Virus Definitions
FORTINET-FORTIGATE-MIB::fgLicVersionDesc.3 = STRING: Extended set
FORTINET-FORTIGATE-MIB::fgLicVersionDesc.4 = STRING: Extreme set
FORTINET-FORTIGATE-MIB::fgLicVersionDesc.5 = STRING: Mobile Malware Definitions
FORTINET-FORTIGATE-MIB::fgLicVersionDesc.6 = STRING: Flow-based Virus Definitions
FORTINET-FORTIGATE-MIB::fgLicVersionDesc.7 = STRING: Botnet Domain Database
FORTINET-FORTIGATE-MIB::fgLicVersionDesc.8 = STRING: Attack Definitions
FORTINET-FORTIGATE-MIB::fgLicVersionDesc.9 = STRING: Attack Extended Definitions
...

```

## IPsec tunnels

New OIDs are added in *fgVpn* to support SNMP query for IPv4 and IPv6 IPsec tunnels, including the following two tables.

#### **fgVpn2DialupTable 1.3.6.1.4.1.12356.101.12.4.1**

```

snmpwalk -v2c -c SNMP-TEST 172.16.200.1 1.3.6.1.4.1.12356.101.12.4.1
FORTINET-FORTIGATE-MIB::fgVpn2DialupIndex.1 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fgVpn2DialupIndex.2 = INTEGER: 2
FORTINET-FORTIGATE-MIB::fgVpn2DialupIndex.3 = INTEGER: 3
FORTINET-FORTIGATE-MIB::fgVpn2DialupIndex.4 = INTEGER: 4
FORTINET-FORTIGATE-MIB::fgVpn2DialupIndex.5 = INTEGER: 5
FORTINET-FORTIGATE-MIB::fgVpn2DialupIndex.6 = INTEGER: 6
FORTINET-FORTIGATE-MIB::fgVpn2DialupGatewayType.1 = INTEGER: ipv6(2)
FORTINET-FORTIGATE-MIB::fgVpn2DialupGatewayType.2 = INTEGER: ipv6(2)
FORTINET-FORTIGATE-MIB::fgVpn2DialupGatewayType.3 = INTEGER: ipv4(1)
FORTINET-FORTIGATE-MIB::fgVpn2DialupGatewayType.4 = INTEGER: ipv4(1)
FORTINET-FORTIGATE-MIB::fgVpn2DialupGatewayType.5 = INTEGER: ipv4(1)
FORTINET-FORTIGATE-MIB::fgVpn2DialupGatewayType.6 = INTEGER: ipv4(1)
...

```

#### **fgVpn2TunTable 1.3.6.1.4.1.12356.101.12.4.2**

```

snmpwalk -v2c -c SNMP-TEST 172.16.200.1 1.3.6.1.4.1.12356.101.12.4.2 (Tunnel VPN)
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.3.1 = STRING: tovd6
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.4.1 = STRING: tovd7
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.6.1 = STRING: dailToVd1
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.7.1 = STRING: vd3-dial-vd1
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.8.1 = STRING: spokel
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.8.2 = STRING: spokel

```

```

FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.9.2 = STRING: spoke1v6
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.9.3 = STRING: spoke1v6
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.10.1 = STRING: Spoke2
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.10.2 = STRING: Spoke2
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.11.1 = STRING: spoke2v6
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.12.1 = STRING: tovd1
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase1Name.13.1 = STRING: vd7to1-ip6
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.3.1 = STRING: tovd6
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.4.1 = STRING: tovd7
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.6.1 = STRING: dailToVd1
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.7.1 = STRING: vd3-to-vd1
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.8.1 = STRING: spoke1
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.8.2 = STRING: spoke1-v2
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.9.2 = STRING: spoke1v6-2
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.9.3 = STRING: spoke1v6
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.10.1 = STRING: Spoke2
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.10.2 = STRING: spoke2-p2
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.11.1 = STRING: spoke2v6
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.12.1 = STRING: tovd1
FORTINET-FORTIGATE-MIB::fgVpn2TunPhase2Name.13.1 = STRING: vd7to1-ip6
FORTINET-FORTIGATE-MIB::fgVpn2TunRemGwyIpType.3.1 = INTEGER: ipv4(1)
FORTINET-FORTIGATE-MIB::fgVpn2TunRemGwyIpType.4.1 = INTEGER: ipv6(2)
FORTINET-FORTIGATE-MIB::fgVpn2TunRemGwyIpType.6.1 = INTEGER: ipv4(1)
...

```

## SNMP OIDs for port block allocations IP pool statistics - 6.4.12

The FortiGate SNMP MIB has been updated to support OIDs that provide data about any configured port block allocation (PBA) IP pools. There are four SNMP OIDs for polling critical PBAs statistics, including total PBAs, in use PBAs, expiring PBAs, and free PBAs:

Name	OID	Description
fgFwIppStatsTotalPBAs	1.3.6.1.4.1.12356.101.5.3.2.1.1.9	The total number of port block allocations.
fgFwIppStatsInusePBAs	1.3.6.1.4.1.12356.101.5.3.2.1.1.10	The number of port block allocations in use.
fgFwIppStatsExpiringPBAs	1.3.6.1.4.1.12356.101.5.3.2.1.1.11	The number of port block allocations that are expiring.
fgFwIppStatsFreePBAs	1.3.6.1.4.1.12356.101.5.3.2.1.1.12	The number of free port block allocations.

For more information about this feature, see [SNMP OIDs for port block allocations IP pool statistics](#).

## FortiGuard

This section includes information about FortiGuard related new features:

- [Use anycast to communicate with FortiGuard servers on page 256](#)
- [IoT detection service on page 258](#)
- [Display cloud service communications statistics on page 260](#)
- [Support third party CA signed certificates with OCSP stapling 6.4.2 on page 261](#)

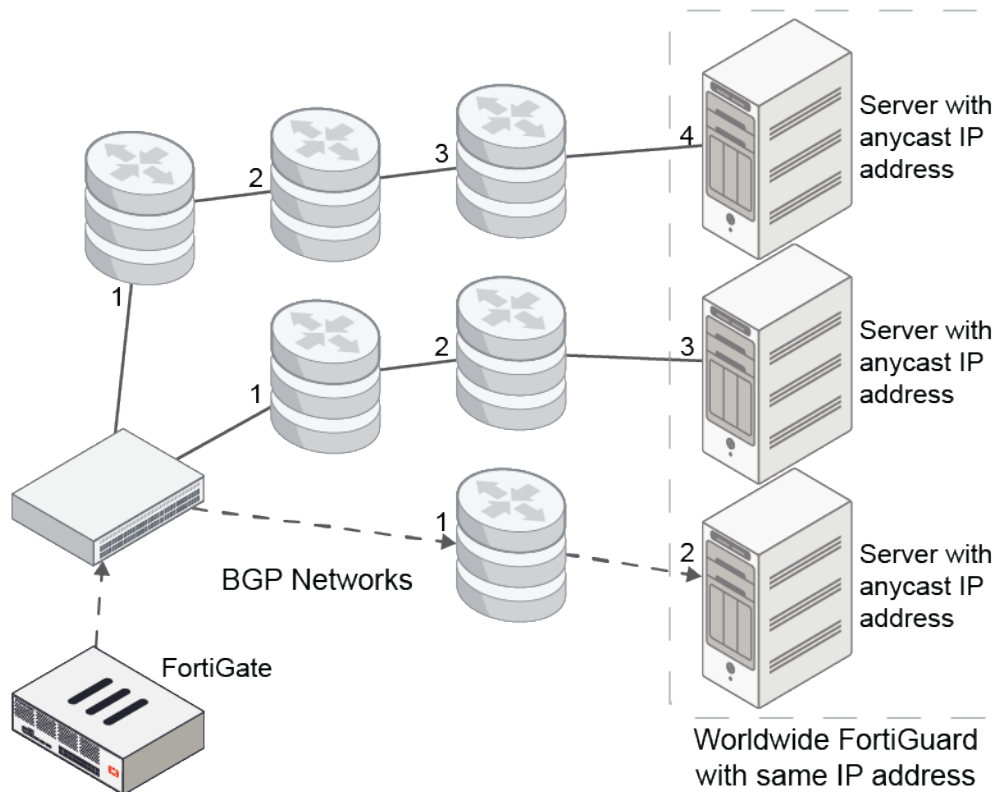
- FDS-only ISDB package in firmware images 6.4.10 on page 261

## Use anycast to communicate with FortiGuard servers

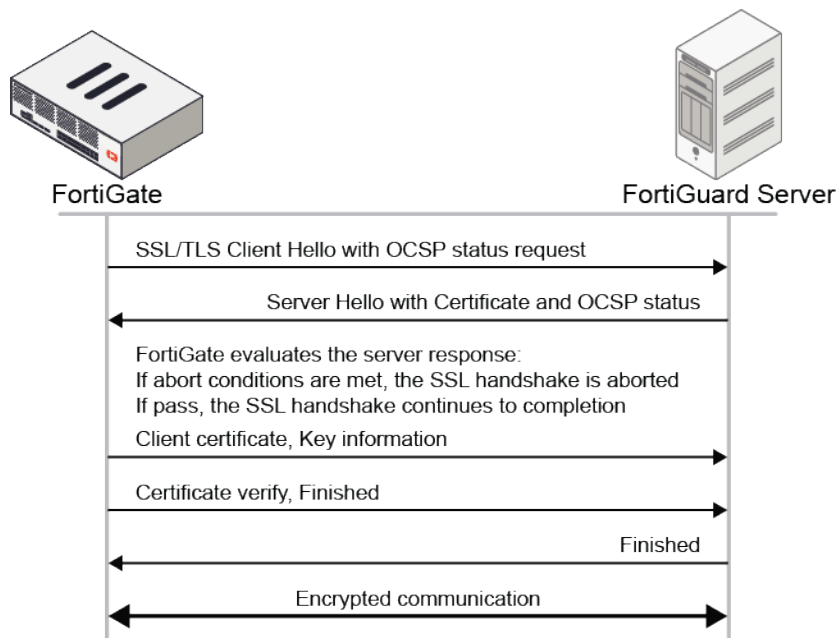
Third party certificate verification and OCSP stapling check is implemented for all FortiGuard servers that are connected to FortiOS. The default FortiGuard access mode is anycast.

FortiGuard represents all cloud based servers; see [Anycast and unicast services](#) for details.

The anycast server has one IP address to match its domain name. The FortiGate connects with a single server address, regardless of where the FortiGate is located.



The following process is used to connect to an anycast server:



Abort conditions include:

- The CN in the server's certificate does not match the domain name resolved from the DNS.
- The OCSP status is not good.
- The issuer-CA is revoked by the root-CA.

Once the SSL handshake is established, the FortiGate can engage the server.

### Example Wireshark PCAP:

```
Time      Source          Destination              Protocol    Length  Info
4.0.001831 10.6.30.102           173.243.140.6            TLSv1.2    381 Client Hello
6.0.02705   173.243.140.6          10.6.30.102             TLSv1.2    1534 Server Hello
10.0.07230  173.243.140.6          10.6.30.102             TLSv1.2    3534 Certificate [TCP segment of a reassembled PDU]
12.0.07418  173.243.140.6          10.6.30.102             TLSv1.2    1108 CertificateStatus, Server Key Exchange, Certificate Request, Server Hello Done
10.0.07583  10.6.30.102           173.243.140.6            TLSv1.2    3534 Certificate, Client Key Exchange
15.0.07586  10.6.30.102           173.243.140.6            TLSv1.2    374 Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
18.0.10207  173.243.140.6          10.6.30.102             TLSv1.2    1534 New Session Ticket, Change Cipher Spec
19.0.10212  173.243.140.6          10.6.30.102             TLSv1.2    3536 Encrypted Handshake Message
20.0.11810  10.6.30.102           173.243.140.6            TLSv1.2    1439 Application Data
22.0.14637  173.243.140.6          10.6.30.102             TLSv1.2    1147 Application Data

Frame 16: 1534 bytes on wire (12112 bits), 1534 bytes captured (12112 bits) on eth0
Ethernet II, Src: Fortinet_53:61:39 (90:6c:ac:53:61:39), Dst: Fortinet_97:c7:b2 (70:6c:a5:97:c7:b2)
Internet Protocol Version 4, Src: 173.243.140.6, Dst: 10.6.30.102
Transmission Control Protocol, Src Port: 443, Dst Port: 15357, Seq: 2897, Ack: 316, Len: 1448
  Reassembled TCP Segments (6244 bytes) (#0:1378), #0(1448), #10(1438)
  Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4239
      Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 4235
        Certificates Length: 4232
        ✓ Certificates (4232 bytes)
          Certificate Length: 2044
          > Certificate: 30a3f3e0d020a00000020020110bf07d0f07ba1459ca... (id-at=commonname-globallupdate.fortinet.net,id-at=organizationName-FORTIGUARD,id-at=organizationName-fortinet)
          Certificate Length: 150
          > Certificate: 30a3f3e0d020a0000002002010bc79a94d040115920... (id-at=commonname-Digicert SHA2 Extended Validation Root CA,id-at=organizationName-digicert.com,id-at=organizationName-digicert-com)
          > Certificate: 30a3f3e0d020a000000200201020ac75a04d000f80... (id-at=commonname-Digicert High Assurance EV Root CA,id-at=organizationName-us.digicert.com,id-at=organizationName-us-digicert-com)
```

**To enable anycast FortiGuard access mode:**

```
config system fortiguard
    set fortiguard-anycast enable
    set fortiguard-anycast-source fortinet
end
```

## IoT detection service

Internet of Things (IoT) detection is a subscription service that allows FortiGate to detect unknown devices in FortiGuard that are not detected by the local Device Database (CIDB). When the service is activated, FortiGate can send device information to the FortiGuard collection server. When a new device is detected, FortiGate queries the results from the FortiGuard query for more information about the device.

This feature requires an IoT Detection Service license.

### FortiGate device requirements:

The FortiGate device must be:

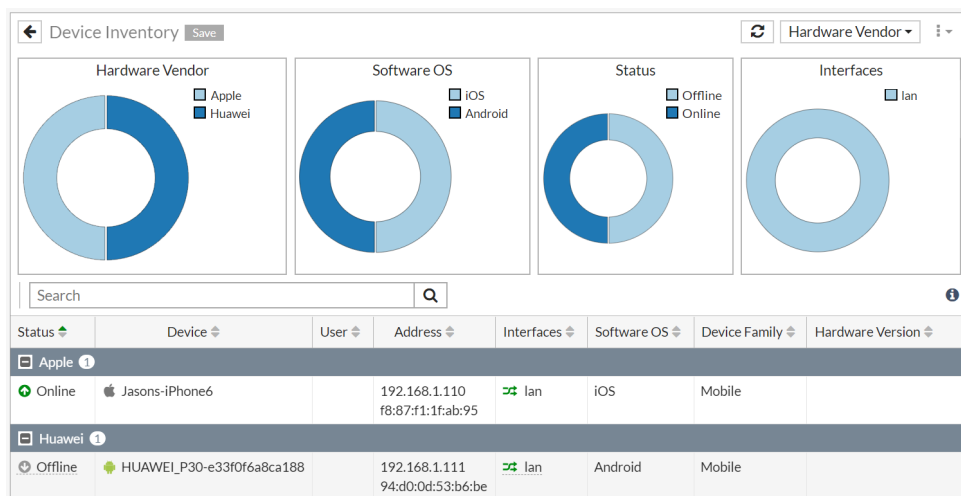
- Registered with FortiCare
- Connected to an anycast FortiGuard server

### How the service works:

1. Enable Device Detection on an interface..
2. FortiGate uses the interface to detect device traffic flow.
3. Upon detecting traffic from an unknown device, FortiGate sends the device data to the FortiGuard collection server.
4. The collection server returns data about the new device to the FortiGuard query server.
5. If the device signature does not appear in the local Device Database (CIDB) or some fields are not complete, FortiGate queries FortiGuard for more information about the device.

## GUI

To view the latest device information in the GUI, go to *Dashboard > Users & Devices* and expand the *Device Inventory* widget.



### To debug the daemon in the CLI:

1. Disable the local device database in order to force all queries to go to FortiGuard.  

```
diagnose src-vis local-sig disable
```



**2. Enable iotd debugs.**

```
diagnose debug application iotd -1
diagnose debug enable
```

**FortiGate sends the device data to the FortiGuard collection server.**

```
FortiWiFi-60E # [iotd] recv request from caller size:61
[iotd] service:collect hostname: ip: fd:-1 request tlv_len:41
[iotd] txt(.....y...w.....Jasons-iPhone6....579=23..)
[iotd] hex
      (02010007017903060f77fc0203000e4a61736f6e732d6950686f6e65536020400083537393d32330cf
      f)
[iotd] service:collect hostname:qadevcollect.fortinet.net ip: fd:-1 got server hostname
[iotd] service:collect hostname:qadevcollect.fortinet.net ip:192.168.100.133 fd:-1 got
      server ip
[iotd] service:collect hostname:qadevcollect.fortinet.net ip:192.168.100.133 fd:13
      socket created
[iotd] service:collect hostname:qadevcollect.fortinet.net ip:192.168.100.133 fd:13
      connecting
[iotd] fd:13 monitor event:pollout
[iotd] service:collect hostname:qadevcollect.fortinet.net ip:192.168.100.133 fd:13 build
      req packet
[iotd] service:collect hostname:qadevcollect.fortinet.net ip:192.168.100.133 fd:13
      collect resp:1(pending)
```

**The FortiGuard collection server returns new device data to the FortiGuard query server.**

```
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17 got query
      resp
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17 id:0
      total_len:48 header_len:16 tlv_len:32 confidence:100 mac:f8:87:f1:1f:ab:95
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17
      remaining_len:32 type:1 len:6
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17 got tlv
      category:'Mobile'
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17
      remaining_len:24 type:2 len:6
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17 got tlv
      sub_category:'Mobile'
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17
      remaining_len:16 type:3 len:5
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17 got tlv
      vendor:'Apple'
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17
      remaining_len:9 type:4 len:0
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17
      remaining_len:7 type:5 len:3
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17 got tlv
      os:'iOS'
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17
      remaining_len:2 type:6 len:0
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17 send
      query response to caller size:48
[iotd] txt(.....d0 ...Mobile..Mobile..Apple....iOS..)
[iotd] hex
      (f887f11fab950000000000000000006430200001064d6f62696c6502064d6f62696c6503054170706c650400
      0503694f530600)
[iotd] service:query hostname:qadevquery.fortinet.net ip:192.168.100.248 fd:17 read
      resp:0(good)
```

**3. The query returns the device information including the information source (src fortiguard).**

```
diagnose user device list
```

```

vd root/0 f8:87:f1:1f:ab:95 gen 26 req OUA/34
created 503s gen 23 seen 102s lan gen 7
ip 192.168.1.110 src arp
hardware vendor 'Apple' src fortiguard id 0 weight 100
type 'Mobile' src fortiguard id 0 weight 100
family 'Mobile' src fortiguard id 0 weight 100
os 'iOS' src fortiguard id 0 weight 100
host 'Jasons-iPhone6' src dhcp

```

## Display cloud service communications statistics

Fortinet service communications statistics are displayed on the *FortiGuard* page. The statistics correspond with the output from `diagnose sys service-communication`. The values for traffic volume in the GUI are sums of data from the last 24 hours.

To view Fortinet service communications statistics:

1. Go to *System > FortiGuard*.

The *Fortinet Service Communications* statistics are displayed on the right-side of the screen:

The screenshot shows the FortiGate 501E GUI. The left sidebar contains the navigation menu with 'System' selected. The main content area is titled 'FortiGuard Distribution Network' and includes a 'License Information' table and a 'Fortinet Service Communications' table.

Entitlement	Status
FortiCare Support	Registered - <a href="#">Launch Portal</a>
Hardware Version	Advanced hardware - expires on 2020/10/02
Enhanced Support	24x7 support - expires on 2020/10/02
Firmware & General Updates	Licensed - expires on 2020/10/02
Application Control Signatures	Version 15.00784 <a href="#">Upgrade Database</a> <a href="#">View List</a>
Device & OS Identification	Version 1.00093
Internet Service Database Definitions	Version 6.00076

Service	Traffic Volume (Last 24 hours)
FortiCare	0 B
FortiCloud Log	150.80 kB
FortiGuard.com	1.06 MB
FortiGuard Download	2.52 MB
FortiGuard Query	15.58 kB
FortiSandbox Cloud	0 B
OCVPN	167.41 kB
SDNS	0 B
FortiToken Registration	0 B
SMS Service	0 B

These statistics correspond to the following:

```

# diagnose sys service-communication
FortiCare:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes): 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  0 0 0 0 0 0 0
FortiGuard Download:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes): 0 0 195752 0 21051904 36342800 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0
The last 7 days(in bytes):  57590456 0 0 0 0 0 0
FortiGuard Query:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes): 0 0 2805 0 1298 1709 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  5812 0 0 0 0 0 0
FortiCloud Log:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0

```

```

The last 24 hours(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):   0 0 0 0 0 0 0
FortiSandbox Cloud:
The last 1 hour(in bytes):   0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes): 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):   0 0 0 0 0 0 0
FortiGuard.com:
The last 1 hour(in bytes):   2014 0 1329 0 1329 0 1329 0 1329 0 2020 103930
The last 24 hours(in bytes): 3343 112595 9032861 18584815 17757745 16054191 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):   61545550 0 0 0 0 0 0
FortiToken Registration:
The last 1 hour(in bytes):   0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes): 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):   0 0 0 0 0 0 0
SMS Service:
The last 1 hour(in bytes):   0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes): 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):   0 0 0 0 0 0 0

```

## Support third party CA signed certificates with OCSP stapling - 6.4.2

FortiGuard servers for GeoIP, DDNS and FortiToken Mobile registration now support third party CA signed certificates with OCSP stapling.

The anycast server has one IP address to match its domain name. The FortiGate connects with a single server address, regardless of where the FortiGate is located.

Service	Non-Anycast FQDN addresses	Anycast Domain name
GeoIP	gip.fortinet.net	globalgip.fortinet.net
DDNS	ddns.fortinet.net	globalddns.fortinet.net
FortiMobile Tokens	directregistration.fortinet.com	globalftm.fortinet.net

See [Anycast and unicast services](#) for details.

## FDS-only ISDB package in firmware images - 6.4.10

FortiOS firmware images include Fortinet objects in the built-in Internet Service Database (ISDB). This lightweight ISDB package allows firewall rules and policy routes that use ISDB to access FortiGuard servers to continue working after upgrading FortiOS.

After the FortiGate reboots after a firmware update, an automatic update will run in five minutes so that the FortiGate can get the ISDB, whether or not scheduled update is enabled.

For more information about this feature, see [FDS-only ISDB package in firmware images](#).

# Policy and Objects

This section includes information about policy and object related new features:

- [Policies on page 262](#)
- [Objects on page 279](#)

## Policies

This section includes information about policy related new features:

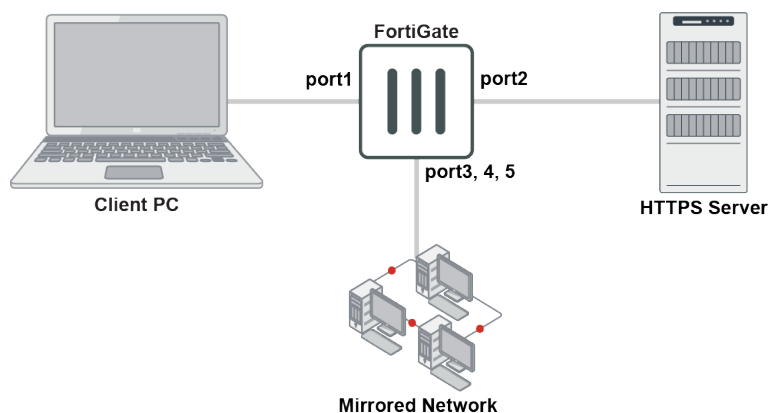
- [Support SSL mirroring in proxy mode on page 262](#)
- [Consolidated IPv4 and IPv6 policy configuration on page 265](#)
- [UUID field added to all policy types on page 267](#)
- [SNAT support for policies with virtual wire pairs on page 269](#)
- [Interface-based traffic shaping with NP acceleration on page 271](#)
- [Ingress traffic shaping profile 6.4.7 on page 273](#)

## Support SSL mirroring in proxy mode

SSL mirroring allows the FortiGate to decrypt and mirror traffic to a designated port. Previously, this was supported in flow mode. Support for proxy mode has been added. A new decrypted traffic mirror profile can be applied to IPv4, IPv6, and explicit proxy firewall policies. Full SSL inspection must be used in the policy for the traffic mirroring to occur.

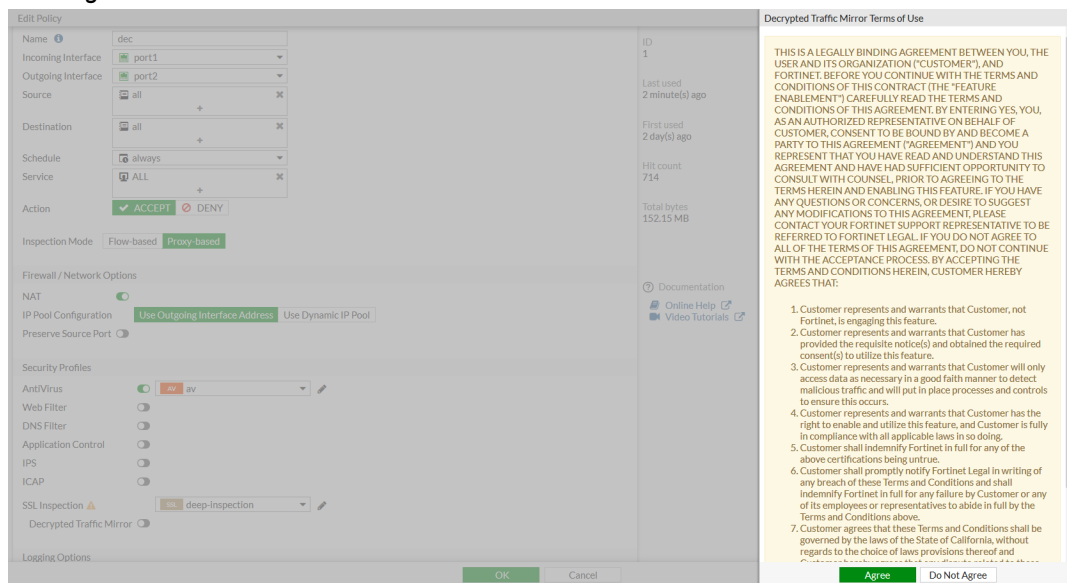


When upgrading to FortiOS 6.4.0, the original `ssl-mirror` and `ssl-mirror-intf` profiles will be replaced with a new `firewall decrypted-traffic-mirror` profile named `__upg_pol_<#>`. The default destination MAC is all FF, and the default source is client.

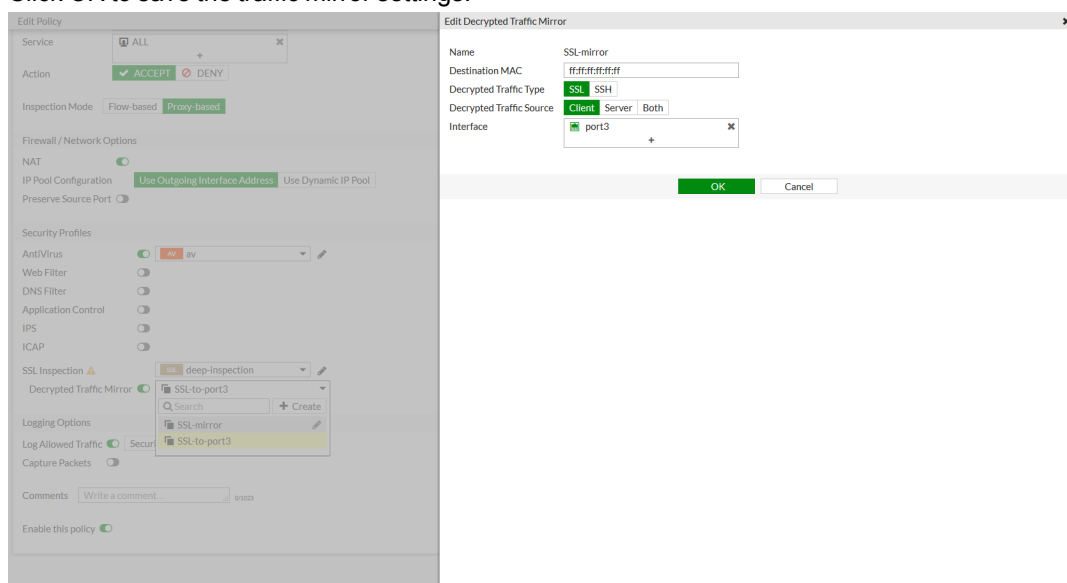


## To configure SSL mirroring in proxy mode in the GUI:

1. Go to *Policy & Objects* and create a new policy, or edit an existing one. This example uses a firewall policy.
2. In the policy settings, ensure the following are configured:
  - a. The *Inspection Mode* is set to *Proxy-based*.
  - b. The *SSL Inspection* profile uses *Full SSL Inspection* (if needed, click the pencil icon next to the dropdown to view the inspection profile settings).
3. Enable the *Decrypted Traffic Mirror* toggle. The terms of use will appear in a separate pane.
4. Click *Agree*.



5. Beside the toggle, click *Create* to configure a new decrypted traffic mirror and adjust the settings as needed. In this example, the client is the decrypted traffic source and port3 is the interface.
6. Click *OK* to save the traffic mirror settings.



7. Click *OK* to save the policy settings.

**To configure SSL mirroring in proxy mode in the CLI:****1. Create the decrypted traffic mirror profile:**

```
config firewall decrypted-traffic-mirror
  edit SSL-to-port3
    set dstmac ff:ff:ff:ff:ff:ff
    set traffic-type ssl
    set traffic-source client
    set interface port3
  next
end
```

**2. Configure the policy to enable SSL traffic mirroring:**

```
config firewall policy
  edit 1
    set inspection-mode proxy
    set ssl-ssh-profile deep-inspection
    set decrypted-traffic-mirror SSL-to-port3
```

THIS IS A LEGALLY BINDING AGREEMENT BETWEEN YOU, THE USER AND ITS ORGANIZATION ("CUSTOMER"), AND FORTINET. BEFORE YOU CONTINUE WITH THE TERMS AND CONDITIONS OF THIS CONTRACT (THE "FEATURE ENABLEMENT") CAREFULLY READ THE TERMS AND CONDITIONS OF THIS AGREEMENT. BY ENTERING YES, YOU, AS AN AUTHORIZED REPRESENTATIVE ON BEHALF OF CUSTOMER, CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT ("AGREEMENT") AND YOU REPRESENT THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT AND HAVE HAD SUFFICIENT OPPORTUNITY TO CONSULT WITH COUNSEL, PRIOR TO AGREEING TO THE TERMS HEREIN AND ENABLING THIS FEATURE. IF YOU HAVE ANY QUESTIONS OR CONCERNS, OR DESIRE TO SUGGEST ANY MODIFICATIONS TO THIS AGREEMENT, PLEASE CONTACT YOUR FORTINET SUPPORT REPRESENTATIVE TO BE REFERRED TO FORTINET LEGAL. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT CONTINUE WITH THE ACCEPTANCE PROCESS. BY ACCEPTING THE TERMS AND CONDITIONS HEREIN, CUSTOMER HEREBY AGREES THAT:

1. Customer represents and warrants that Customer, not Fortinet, is engaging this feature.

2. Customer represents and warrants that Customer has provided the requisite notice(s) and obtained the required consent(s) to utilize this feature.

3. Customer represents and warrants that Customer will only access data as necessary in a good faith manner to detect malicious traffic and will put in place processes and controls to ensure this occurs.

4. Customer represents and warrants that Customer has the right to enable and utilize this feature, and Customer is fully in compliance with all applicable laws in so doing.

5. Customer shall indemnify Fortinet in full for any of the above certifications being untrue.

6. Customer shall promptly notify Fortinet Legal in writing of any breach of these Terms and Conditions and shall indemnify Fortinet in full for any failure by Customer or any of its employees or representatives to abide in full by the Terms and Conditions above.

7. Customer agrees that these Terms and Conditions shall be governed by the laws

of the State of California, without regards to the choice of laws provisions thereof and Customer hereby agrees that any dispute related to these Terms and Conditions shall be resolved in Santa Clara County, California, USA, and Customer hereby consents to personal jurisdiction in Santa Clara County, California, USA.

```

Do you want to continue? (y/n)y
next
end

```

## Consolidated IPv4 and IPv6 policy configuration

IPv4 and IPv6 policy configuration are consolidated in both NGFW profile-based and NGFW policy-based modes. When creating a policy, both IPv4 and IPv6 addresses can be added as sources and destinations.

The IP version of the sources and destinations in a policy must match. For example, a policy cannot have only an IPv4 source and an IPv6 destination.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	IP Version
34		port4	port1	all all6	all all6	always	ALL	ACCEPT Enabled	Enabled	no-inspection	IPv4 + IPv6
44		port4	port3	all all6	all all6	always	ALL	ACCEPT Enabled	Disabled	certificate-inspection	All
99		port3	port1	all all6	all all6	always	ALL	ACCEPT Enabled	Enabled	no-inspection	UTM
91		port2	port2	all all6	all all6	always	ALL	ACCEPT Enabled	Enabled	no-inspection	UTM
222		port2	port1	all all6	all all6	always	ALL	ACCEPT Enabled	Enabled	certificate-inspection	UTM
0	Implicit Deny	any	any	all all6	all all6	always	ALL	DENY	Disabled		Disabled

The policy list can be filtered to show policies with IPv4, IPv6, or IPv4 and IPv6 sources and destinations.

When upgrading from FortiOS 6.2.3 and later to 6.4.0 and later:

- In NGFW profile-based mode, IPv4 and IPv6 policies will all be added to the Firewall Policy list, with IPv6 policies listed after IPv4 policies. If consolidated policy mode is enabled, consolidated policies will be changed to firewall policies.
- In NGFW policy-based mode, policies will be changed from consolidated policies to firewall policies in the CLI.
- The `config firewall policy6` and `config firewall consolidated policy` commands, and the `consolidated-firewall-mode` variable in the `config system settings` command, are all removed.



By default, IPv6 options are not visible. See [Feature visibility](#) for instructions on making them visible.

## NGFW Profile-based mode

To configure an IPv4 and IPv6 firewall policy in the CLI:

```

config firewall policy
edit 99
set srcintf "port3"
set dstintf "port1"

```

```
set srcaddr "all"
set dstaddr "all"
set srcaddr6 "all6"
set dstaddr6 "all6"
set action accept
set schedule "always"
set service "ALL"
set nat enable
set ippool enable
set poolname "ipv4-ippool-1"
set poolname6 "ipv6-ippool-1"
next
end
```

**To check the iprope lists for the policy:**

```
# diagnose firewall iprope list 100004
policy index=99 uuid_idx=56 action=accept
flag (8050108): redir nat master use_src pol_stats
flag2 (4000): resolve_sso
flag3 (20): link-local
schedule(always)
cos_fwd=255 cos_rev=255
group=00100004 av=00004e20 au=00000000 split=00000000
host=1 chk_client_info=0x0 app_list=0 ips_view=0
misc=0
zone(1): 11 -> zone(1): 9
source(1): 0.0.0.0-255.255.255.255, uuid_idx=21,
dest(1): 0.0.0.0-255.255.255.255, uuid_idx=21,
service(1):
    [0:0x0:0/(0,65535)->(0,65535)] helper:auto
nat(1): flag=1 base=0.0.0.0:0 2.2.2.30-2.2.2.40(0:0)

# diagnose firewall iprope6 list 100004
policy id: 99, group: 00100004, uuid_idx=56
  action: accept, schedule: always
  cos_fwd=255 cos_rev=255
  flag (08050108): redir nat master use_src pol_stats
  flag2(00004000): resolve_sso
  shapers: / per_ip=
  sub_groups: av 00004e20 auth 00000000 split 00000000 misc 00000000
  app_list: 0 ips_view: 0
  vdom_id: 1
  zone_from(1): 11
  zone_to(1): 9
  address_src(1):
    all uuid_idx=40
  address_dst(1):
    all uuid_idx=40
  service(1):
    [0:0x0:0/(0,65535)->(0,65535)] helper:auto
nat(1):
  flag=1 base=::(:0)
  2003::2003 - 2003::2004(0:0)
```



## NGFW Policy-based mode

### To configure an IPv4 and IPv6 SSL Inspection & Authentication policy in the CLI:

```
config firewall policy
  edit 2
    set srcintf "port24"
    set dstintf "port17"
    set srcaddr "all"
    set dstaddr "all"
    set srcaddr6 "all"
    set dstaddr6 "all"
    set service "ALL"
    set auto-asic-offload disable
  next
end
```

### To configure an IPv4 and IPv6 security policy in the CLI:

```
config firewall security-policy
  edit 1
    set comments "test"
    set srcintf "port24"
    set dstintf "port17"
    set srcaddr "all"
    set dstaddr "all"
    set srcaddr6 "all"
    set dstaddr6 "all"
    set enforce-default-app-port disable
    set service "ALL"
    set action accept
    set schedule "always"
    set logtraffic all
  next
end
```

## UUID field added to all policy types

The UUID field has been added to all policy types, including multicast, local-in (IPv4 and IPv6), and central SNAT policies. UUIDs are automatically generated by FortiOS when the policy is created and can be viewed in the CLI using the `show` command.

A comments field has also been added for multicast policies.

### To view the UUID for a multicast policy:

#### 1. Create a policy:

```
config firewall multicast-policy
  edit 1
    set comments "multicast-policy-1"
    set logtraffic enable
    set srcintf "wan1"
    set dstintf "wan2"
```

```
        set srcaddr "all"
        set dstaddr "230-0-0-1" "test-multicast-addr-1"
        set snat enable
        set snat-ip 10.1.100.188
        set dnat 229.1.2.19
        set auto-asic-offload disable
    next
end
```

## 2. Use the show command to see the UUID:

```
# show firewall multicast-policy
config firewall multicast-policy
edit 1
    set uuid d0f74f64-fc41-51e9-2dfc-729f027e9979
    set comments "multicast-policy-1"
    set logtraffic enable
    set srcintf "wan1"
    set dstintf "wan2"
    set srcaddr "all"
    set dstaddr "230-0-0-1" "test-multicast-addr-1"
    set snat enable
    set snat-ip 10.1.100.188
    set dnat 229.1.2.19
    set auto-asic-offload disable
next
end
```

## To view the UUID for an IPv4 or IPv6 local-in policy:

### 1. Create a policy:

```
config firewall local-in-policy
edit 1
    set intf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set service "PING"
    set schedule "always"
    set comments "test-1"
next
end
```

### 2. Use the show command to see the UUID:

```
# show firewall local-in-policy
config firewall local-in-policy
edit 1
    set uuid 1aeb7d98-0016-51ea-7913-b6d62f4409cd
    set intf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set service "PING"
    set schedule "always"
    set comments "test-1"
```

```
    next
end
```

### To view the UUID for a central SNAT policy:

#### 1. Create a policy:

```
config firewall central-snat-map
    edit 1
        set srcintf "wan2"
        set dstintf "wan1"
        set orig-addr "all"
        set dst-addr "all"
        set orig-port 11111
        set nat-ippool "Overload-ippool-1"
        set nat-port 22222
    next
end
```

#### 2. Use the show command to see the UUID:

```
# show firewall central-snat-map
config firewall central-snat-map
    edit 1
        set uuid d0f87af6-fc41-51e9-ef72-32f8655f8008
        set srcintf "wan2"
        set dstintf "wan1"
        set orig-addr "all"
        set dst-addr "all"
        set orig-port 11111
        set nat-ippool "Overload-ippool-1"
        set nat-port 22222
    next
end
```

## SNAT support for policies with virtual wire pairs

Source NAT (SNAT) can be configured in IPv4 and IPv6 policies with virtual wire pair (VWP) interfaces, and between VWP interfaces when central NAT is enabled.

### To configure a policy using SNAT and a VWP interface when central NAT is disabled:

#### 1. Create the VWP interface:

```
config system virtual-wire-pair
    edit "test-vw-1"
        set member "port1" "port4"
    next
end
```

#### 2. Create the IP pool. The IP pool must have a different subnet than the VWP peers.

```
config firewall ippool
    edit "vwp-pool-1"
        set startip 172.16.222.99
        set endip 172.16.222.100
```

```
    next
end
```

### 3. Configure the firewall policy:

```
config firewall policy
    edit 88
        set srcintf "port4"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
        set ippool enable
        set poolname "vwp-pool-1"
    next
end
```

### 4. Verify the IP pool functions as expected and traffic passes through:

```
# diagnose sniffer packet any icmp 4
interfaces=[any]
filters=[icmp]
23.438095 port4 in 172.16.200.11 -> 172.16.200.156: icmp: echo request
23.438126 port1 out 172.16.222.100 -> 172.16.200.156: icmp: echo request
23.438492 port1 in 172.16.200.156 -> 172.16.222.100: icmp: echo reply
23.438501 port4 out 172.16.200.156 -> 172.16.200.11: icmp: echo reply
24.439305 port4 in 172.16.200.11 -> 172.16.200.156: icmp: echo request
24.439319 port1 out 172.16.222.100 -> 172.16.200.156: icmp: echo request
24.439684 port1 in 172.16.200.156 -> 172.16.222.100: icmp: echo reply
24.439692 port4 out 172.16.200.156 -> 172.16.200.11: icmp: echo reply

8 packets received by filter
0 packets dropped by kernel
```

## To configure a SNAT between VWP interfaces when central NAT is enabled:

### 1. Enable central NAT:

```
config system settings
    set central-nat enable
end
```

### 2. Create the VWP interface:

```
config system virtual-wire-pair
    edit "test-vw-1"
        set member "port1" "port4"
    next
end
```

### 3. Create the IP pool. The IP pool must have a different subnet than the VWP peers.

```
config firewall ippool
    edit "vwp-pool-1"
        set startip 172.16.222.99
```

```
        set endip 172.16.222.100
    next
end
```

#### 4. Configure the SNAT policy:

```
config firewall central-snat-map
    edit 2
        set srcintf "port4"
        set dstintf "port1"
        set orig-addr "all"
        set dst-addr "all"
        set nat-ippool "vwp-pool-1"
    next
end
```

#### 5. Configure the firewall policy:

```
config firewall policy
    edit 90
        set srcintf "port4"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

## Interface-based traffic shaping with NP acceleration

Interface-based traffic shaping with NP acceleration is supported on some devices.

An administrator configures the WAN interface's maximum outbound bandwidth and, based on that, creates a traffic shaping profile with a percentage based shaper. This allows for proper QoS and traffic shaping. VLAN interfaces are not supported.

This feature is supported on FortiGate 600E, 500E, and 300E models.

### To configure interface-based traffic shaping:

#### 1. Enable NPU offloading when doing interface-based traffic shaping according to the egress-shaping-profile:

```
config system npu
    set intf-shaping-offload enable
end
```

#### 2. Configure shaping profiles:

```
config firewall shaping-profile
    edit "sdwan"
        set default-class-id 4
        config shaping-entries
            edit 1
                set class-id 4
            next
        next
    next
end
```

```
        set guaranteed-bandwidth-percentage 3
        set maximum-bandwidth-percentage 5
    next
    edit 2
        set class-id 3
        set priority medium
        set guaranteed-bandwidth-percentage 50
        set maximum-bandwidth-percentage 100
    next
    edit 3
        set class-id 2
        set priority low
        set guaranteed-bandwidth-percentage 1
        set maximum-bandwidth-percentage 5
    next
end
next
end
```

The class number is limited to 16.

### 3. Configure a traffic shaper and shaping policy:

```
config firewall shaper traffic-shaper
    edit "Transactional"
        set priority medium
    next
end

config firewall shaping-policy
    edit 1
        set service "ALL"
        set dstintf "any"
        set traffic-shaper "Transactional"
        set class-id 3
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

### 4. Apply the egress shaping profile on the interface:

```
config system interface
    edit "port2"
        set vdom "root"
        set ip 10.1.100.23 255.255.255.0
        set allowaccess ping
        set type physical
        set outbandwidth 500
        set egress-shaping-profile "sdwan"
        set snmp-index 4
    next
end
```

### 5. Configure a firewall policy:

```
config firewall policy
    edit 3
        set srcintf "port2"
```

```

        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end

```

## Ingress traffic shaping profile - 6.4.7

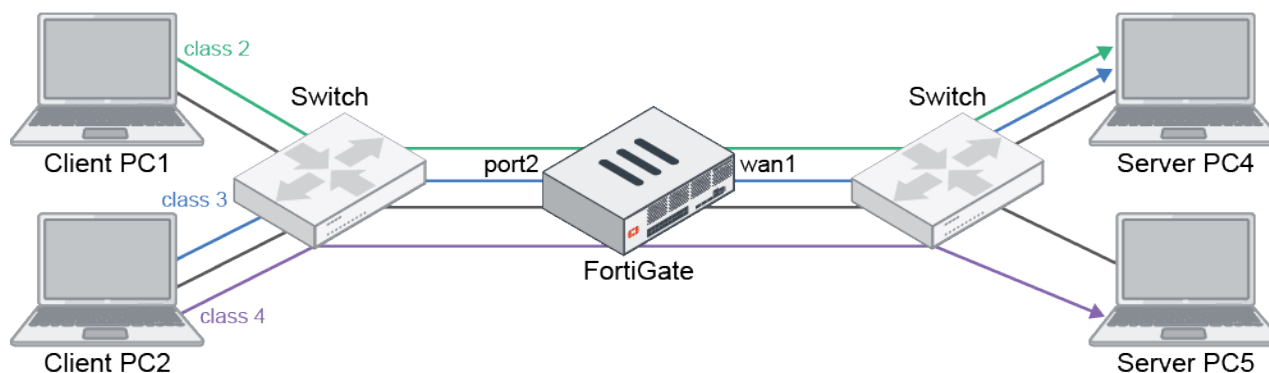
Previously, traffic shaping using a shaping profile could only be applied to an interface in the egress traffic direction. This feature enables a shaping profile to be applied to an interface for traffic in the ingress direction. Similar to an egress traffic shaping profile, the guaranteed bandwidth and priority of the profile will be respected when an interface receives inbound traffic. When congestion occurs, any remaining bandwidth will be allotted to classes based on priority.



Ingress traffic shaping does not support NPU offloading.

### Example

In this example, the port2 interface has a total inbound bandwidth of 100 Mbps. Traffic from certain clients to certain servers are assigned different classes.



IPv6 traffic from any client PCs to server PCs is assigned class 5.

For each class, the priority, guaranteed bandwidth, and maximum bandwidth are as follows:

Class	Priority	Guaranteed bandwidth	Maximum bandwidth
2	Low	10%	60%
3	High	20%	100%
4	High	30%	100%
5	Medium	10%	50%

Bandwidth will first be allotted to each class according to its guaranteed bandwidth. Then remaining available bandwidth will be allotted to class 3 and 4 first based on their priority. The allocation will be proportional to their guaranteed bandwidth ratio.

### To configure ingress traffic shaping:

#### 1. Configure the client and server addresses:

```
config firewall address
  edit "pc1"
    set subnet 10.1.100.11 255.255.255.255
  next
  edit "pc2"
    set subnet 10.1.100.22 255.255.255.255
  next
  edit "pc4"
    set subnet 172.16.200.44 255.255.255.255
  next
  edit "pc5"
    set subnet 172.16.200.55 255.255.255.255
  next
end
```

#### 2. Configure the class IDs:

```
config firewall traffic-class
  edit 2
    set class-name "class2"
  next
  edit 3
    set class-name "class3"
  next
  edit 4
    set class-name "class4"
  next
  edit 4
    set class-name "class5"
  next
end
```

#### 3. Configure traffic shaping policies to assign classes to each group of traffic.

##### a. Configure a policy to assign traffic from PC1 to PC4 in class 2:

```
config firewall shaping-policy
  edit 1
    set name "shaping policy 1"
    set service "ALL"
    set dstintf "wan1"
    set class-id 2
    set srcaddr "pc1"
    set dstaddr "pc4"
  next
end
```

##### b. Configure a policy to assign traffic from PC2 to PC4 in class 3:

```
config firewall shaping-policy
  edit 2
```



```
        set name "shaping policy 2"
        set service "ALL"
        set dstintf "wan1"
        set class-id 3
        set srcaddr "pc2"
        set dstaddr "pc4"
    next
end
```

**c. Configure a policy to assign traffic from PC2 to PC5 in class 4:**

```
config firewall shaping-policy
    edit 3
        set name "shaping policy 3"
        set service "ALL"
        set dstintf "wan1"
        set class-id 4
        set srcaddr "pc2"
        set dstaddr "pc5"
    next
end
```

**d. Configure a policy to assign all IPv6 traffic to class 5:**

```
config firewall shaping-policy
    edit 4
        set name "shaping policy 4"
        set ip-version 6
        set service "ALL"
        set dstintf "wan1"
        set class-id 5
        set srcaddr6 "all"
        set dstaddr6 "all"
    next
end
```

**4. Configure a shaping profile to set the priority, and the guaranteed and maximum bandwidth percentages for each class:**

```
config firewall shaping-profile
    edit "ingShapeProfile"
        set default-class-id 2
        config shaping-entries
            edit 2
                set class-id 2
                set priority low
                set guaranteed-bandwidth-percentage 10
                set maximum-bandwidth-percentage 60
            next
            edit 3
                set class-id 3
                set guaranteed-bandwidth-percentage 20
                set maximum-bandwidth-percentage 100
            next
            edit 4
                set class-id 4
                set guaranteed-bandwidth-percentage 30
                set maximum-bandwidth-percentage 100
        
```

```
        next
        edit 5
            set class-id 5
            set priority medium
            set guaranteed-bandwidth-percentage 10
            set maximum-bandwidth-percentage 50
        next
    end
next
end
```

**5. Configure the inbandwidth and apply the ingress shaping profile on port2:**

```
config system interface
    edit "port2"
        set ip 10.1.100.1 255.255.255.0
        set inbandwidth 100000
        set ingress-shaping-profile "ingShapeProfile"
        config ipv6
            set ip6-address 2000:10:1:100::1/64
        end
    next
end
```

Inbandwidth must be configured for traffic shaping to take effect.

**6. Configure a firewall policy to allow traffic to go through. Since traffic shaping is for inbound traffic on port2, the policy is defined from port2 to wan1:**

```
config firewall policy
    edit 2
        set srcintf "port2"
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end
```

NPU must be disabled by configuring `set auto-asic-offload disable`.

## Verifying that the traffic is being shaped

In each of the following cases, the server PCs (PC4 and PC5) are configured as iPerf servers. The client PCs (PC1 and PC2) are configured as iPerf clients. The client sends traffic to the server from the client to server direction, triggering inbound traffic shaping on the port2 interface. The inbound bandwidth on port2 is 100 Mbps.

### Case 1: single stream, PC1 to PC4

Traffic is sent from PC1 to PC4. There is no other traffic. Traffic is marked with class ID 2 and allocated the maximum bandwidth 60 Mbps (60%).

```
# diagnose netlink interface list port2
if=port2 family=00 type=1 index=20 mtu=1500 link=0 master=0
ref=25 state=start present fw_flags=3800 flags=up broadcast run multicast
Qdisc=mq hw_addr=70:4c:a5:7d:d4:95 broadcast_addr=ff:ff:ff:ff:ff:ff
ingress traffic control:
    bandwidth=100000 (kbps) lock_hit=50 default_class=2 n_active_class=4
    class-id=2 allocated-bandwidth=60000 (kbps) guaranteed-bandwidth=10000
(kbps)
        max-bandwidth=60000 (kbps) current-bandwidth=60002 (kbps)
        priority=low forwarded_bytes=58157K
        dropped_packets=94K dropped_bytes=125385K
    class-id=5 allocated-bandwidth=1000 (kbps) guaranteed-bandwidth=10000 (kbps)
        max-bandwidth=50000 (kbps) current-bandwidth=0 (kbps)
        priority=medium forwarded_bytes=0
        dropped_packets=0 dropped_bytes=0
    class-id=3 allocated-bandwidth=15000 (kbps) guaranteed-bandwidth=20000
(kbps)
        max-bandwidth=100000 (kbps) current-bandwidth=0 (kbps)
        priority=high forwarded_bytes=0
        dropped_packets=0 dropped_bytes=0
    class-id=4 allocated-bandwidth=24000 (kbps) guaranteed-bandwidth=30000
(kbps)
        max-bandwidth=100000 (kbps) current-bandwidth=0 (kbps)
        priority=high forwarded_bytes=0
        dropped_packets=0 dropped_bytes=0
stat: rxp=173465879 txp=2430534 rxb=194665548609 txb=2767375732 rxe=0 txe=0 rxd=0 txd=0 mc=0
collision=0 @ time=1628814469
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=25
```

## Case 2: dual stream, PC1 to PC4, PC2 to PC4

Traffic is sent from both PC1 and PC2 to PC4. PC1 to PC4 traffic is marked with class ID 2 and low priority, and PC2 to PC4 traffic is marked with class ID 3 and high priority. Both class 2 and 3 will be allocated their guaranteed bandwidth first, using up 10% and 20% respectively. The remaining available bandwidth is used by class 3 since it has a higher priority. Class 2 uses around 10 Mbps, and class 3 uses around 90 Mbps.

```
# diagnose netlink interface list port2
if=port2 family=00 type=1 index=20 mtu=1500 link=0 master=0
ref=36 state=start present fw_flags=3800 flags=up broadcast run multicast
Qdisc=mq hw_addr=70:4c:a5:7d:d4:95 broadcast_addr=ff:ff:ff:ff:ff:ff
ingress traffic control:
    bandwidth=100000 (kbps) lock_hit=181 default_class=2 n_active_class=4
    class-id=2 allocated-bandwidth=10000 (kbps) guaranteed-bandwidth=10000
(kbps)
        max-bandwidth=60000 (kbps) current-bandwidth=10001 (kbps)
        priority=low forwarded_bytes=1799482K
        dropped_packets=5998K dropped_bytes=7965553K
    class-id=5 allocated-bandwidth=1000 (kbps) guaranteed-bandwidth=10000 (kbps)
        max-bandwidth=50000 (kbps) current-bandwidth=0 (kbps)
        priority=medium forwarded_bytes=0
        dropped_packets=0 dropped_bytes=0
    class-id=3 allocated-bandwidth=88000 (kbps) guaranteed-bandwidth=20000
(kbps)
```

```

max-bandwidth=100000 (kbps)      current-bandwidth=88000 (kbps)
priority=high    forwarded_bytes=345039K
dropped_packets=324K    dropped_bytes=430862K
class-id=4    allocated-bandwidth=1000 (kbps)    guaranteed-bandwidth=30000 (kbps)
max-bandwidth=100000 (kbps)      current-bandwidth=0 (kbps)
priority=high    forwarded_bytes=0
dropped_packets=0    dropped_bytes=0
stat: rxp=181269891 txp=2433428 rxb=205136511596 txb=2771214402 rxe=0 txe=0 rxd=0 txd=0 mc=0
collision=0 @ time=1628815849
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=36

```

### Case 3: multiple streams

Multiple streams of traffic are sent at the same time:

- PC1 to PC4 traffic is assigned class 2 with low priority, and a guaranteed bandwidth of 10 Mbps.
- PC2 to PC4 traffic is assigned class 3 with high priority, and a guaranteed bandwidth of 20 Mbps.
- PC2 to PC5 traffic is assigned class 4 with high priority, and a guaranteed bandwidth of 30 Mbps.

All classes will be allocated their guaranteed bandwidth first, using up 10 Mbps, 20 Mbps, and 30 Mbps respectively. The remaining available bandwidth (40 Mbps) is shared by class 3 and class 4 based on their guaranteed bandwidth ratio of 20:30.

- Class 3's share of the remaining 40 Mbps traffic =  $40 \times 20 / (20 + 30) = 16$  Mbps
- Class 4's share of the remaining 40 Mbps traffic =  $40 \times 30 / (20 + 30) = 24$  Mbps

Each class is allocated roughly the following bandwidth:

- Class 2: 10 Mbps
- Class 3: 20 Mbps + 16 Mbps = 36 Mbps
- Class 4: 30 Mbps + 24 Mbps = 54 Mbps

```

# diagnose netlink interface list port2
if=port2 family=00 type=1 index=20 mtu=1500 link=0 master=0
ref=27 state=start present fw_flags=3800 flags=up broadcast run multicast
Qdisc=mq hw_addr=70:4c:a5:7d:d4:95 broadcast_addr=ff:ff:ff:ff:ff:ff
ingress traffic control:
    bandwidth=100000 (kbps) lock_hit=148731 default_class=2 n_active_class=4
    class-id=2    allocated-bandwidth=10000 (kbps)    guaranteed-bandwidth=10000
(kbps)
max-bandwidth=60000 (kbps)      current-bandwidth=10004 (kbps)
priority=low    forwarded_bytes=2267956K
dropped_packets=10389K    dropped_bytes=13796469K
class-id=5    allocated-bandwidth=1000 (kbps)    guaranteed-bandwidth=10000 (kbps)
max-bandwidth=50000 (kbps)      current-bandwidth=0 (kbps)
priority=medium    forwarded_bytes=0
dropped_packets=0    dropped_bytes=0
class-id=3    allocated-bandwidth=35000 (kbps)    guaranteed-bandwidth=20000
(kbps)
max-bandwidth=100000 (kbps)      current-bandwidth=35729 (kbps)
priority=high    forwarded_bytes=2119502K
dropped_packets=6020K    dropped_bytes=7994926K
class-id=4    allocated-bandwidth=54000 (kbps)    guaranteed-bandwidth=30000
(kbps)

```

```
max-bandwidth=100000 (kbps)      current-bandwidth=53907 (kbps)
priority=high    forwarded_bytes=902415K
dropped_packets=4141K    dropped_bytes=5499248K
stat: rxp=197827723 txp=2433885 rxb=227356779526 txb=2771602657 rxe=0 txe=0 rxd=0 txd=0 mc=0
collision=0 @ time=1628816440
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=27
```

## Objects

This section includes information about object related new features:

- [Array structure for address objects on page 279](#)
- [Allow creation of ISDB objects with regional information on page 281](#)
- [IP definitions database merged into the internet service database on page 283](#)
- [Extend ISDB to include well-known MAC address list on page 285](#)
- [GeoIP matching by registered and physical location on page 286](#)
- [Group address objects synchronized from FortiManager on page 288](#)
- [Increase in maximum number of VIP real servers on page 290](#)
- [GUI support for real server configurations using address objects 6.4.2 on page 290](#)

### Array structure for address objects

Some address objects logically belong to the same device, such as two IPs from the same computer. These address objects can be grouped into an address folder, which is an exclusive list of address objects that do not appear in other address groups or folders.

In the CLI, the folder type can be set after the member list is already populated. If the member list contains an incompatible entry, then the setting will be discarded when the `next/end` command is issued. If the folder type is set before the member list is populated, then the possible member entry list will be filtered according to the selected type.

#### To create an address folder in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address Group* and enter a name.
3. For *Type*, select *Folder*.
4. For *Members*, click the + to add the addresses. Address folders and groups are exclusive, so the *Select Entries* window filters out address objects that are a member of an existing group or folder.

**New Address Group**

Group name: dev1-addr-comb

Color: Members of address folders can only belong to a single address folder.

Type: Group Folder

Members:

- dev1-IP-nic1
- dev1-IP-nic2
- dev1-mac

Static route configuration: ☐

Comments:  0/255

- Click **OK**.
- In the address table, expand the **Address Group** section to view the folder (*dev1-addr-comb*). The expandable folder view shows the address folder's child objects:

safe-network1-devices	Address Group (Folder)	2 entries	0
dev1-addr-comb	Address Group (Folder)	3 entries	1
dev1-IP-nic1	Subnet	192.168.1.25/32	1
dev1-IP-nic2	Subnet	192.168.1.22/32	1
dev1-mac	Device (MAC Address)	00:0a:95:9d:68:16	1
dev2-addr-comb	Address Group (Folder)	4 entries	1
dev2-IP-nic1	Subnet	192.168.1.101/32	1
dev2-IP-nic2	Subnet	192.168.1.102/32	1
dev2-IP-nic3	Subnet	192.168.1.103/32	1
dev2-mac	Device (MAC Address)	11:5b:12:2c:87:02	1

### To configure an address folder in the CLI:

#### notes

```

config firewall addrgrp
    edit "safe-network1-devices"
        set type folder
        set member "dev1-addr-comb" "dev2-addr-comb"
        set comment ''
        set exclude disable
        set color 13
    next
end

config firewall addrgrp
    edit "dev1-addr-comb"
        set type folder
        set member "dev1-IP-nic1" "dev1-IP-nic2" "dev1-mac"
        set comment ''
        set exclude disable
        set color 18
    next
end

```

```

config firewall addrgrp
  edit "dev2-addr-comb"
    set type folder
    set member "dev2-IP-nic1" "dev2-IP-nic2" "dev2-IP-nic3" "dev2-mac"
    set comment ''
    set exclude disable
    set color 5
  next
end

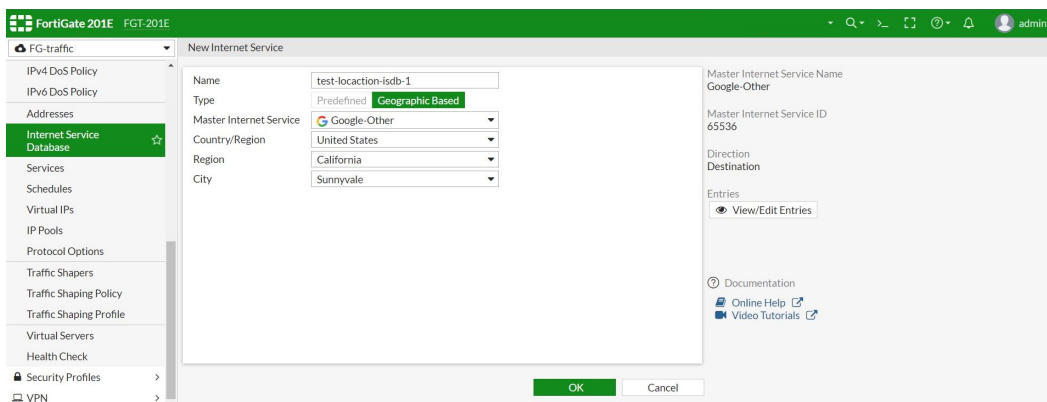
```

## Allow creation of ISDB objects with regional information

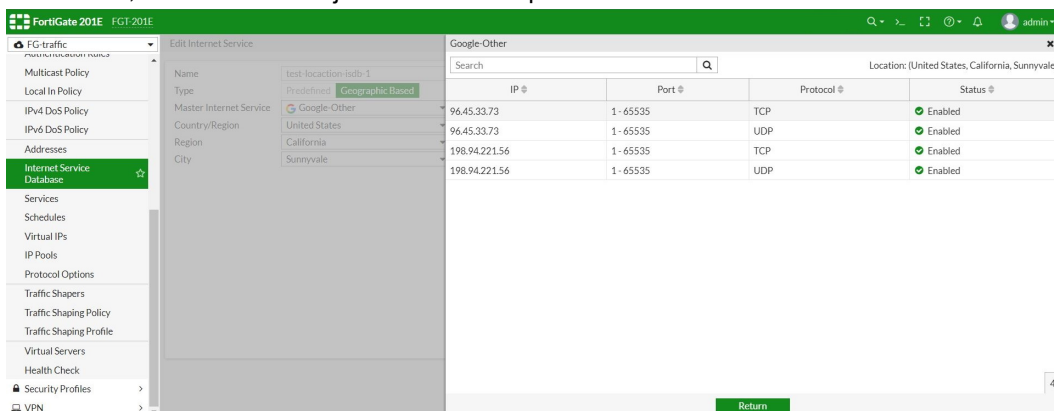
Geographic-based Internet Service Database (ISDB) objects allow users to define a country, region, and city. These objects can be used in firewall policies for more granular control over the location of the parent ISDB object. ISDB objects are now referenced in policies by name instead of ID.

### To apply a location-based ISDB object to a policy in the GUI:

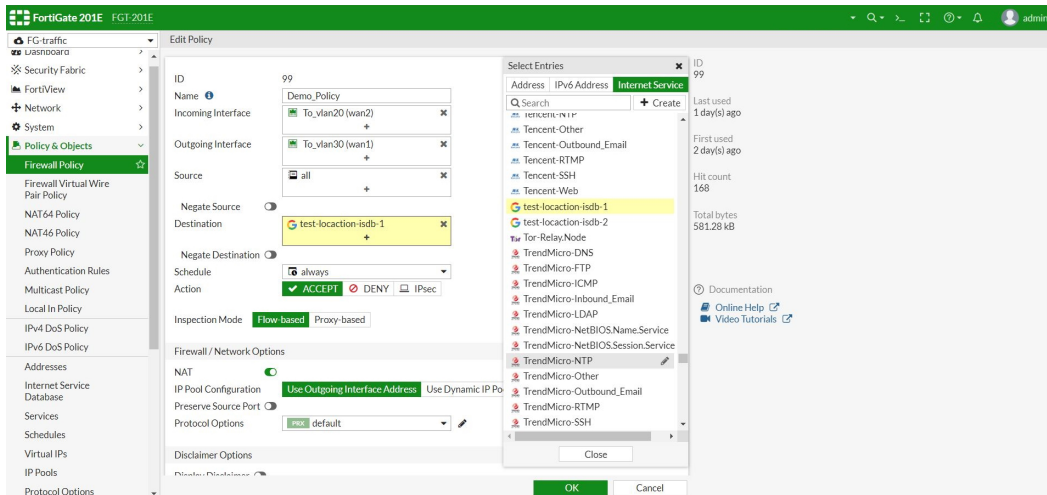
1. Create the ISDB object:
  - a. Go to *Policy & Objects > Internet Service Database > Create New*.
  - b. For *Type*, select *Geographic Based*, and configure the other settings as needed.
  - c. Click *OK*.



2. View the IP ranges in the location-based internet service:
  - a. Go to *Policy & Objects > Internet Service Database*.
  - b. In the table, hover over the object created in step 1 and click *View/Edit Entries*. The list of IPs is displayed:



- c. Click *Return*.
3. Add the ISDB object to a policy:
  - a. Go to *Policy & Objects > Firewall Policy*. Create a new policy or edit an existing policy.
  - b. For *Destination*, click *Internet Service* and select the ISDB object created in step 1.
  - c. Configure the other settings as needed.



- d. Click *OK*.

### To apply a location-based ISDB object to a policy in the CLI:

1. Create the ISDB object:

```
config firewall internet-service-name
  edit "test-location-isdb-1"
    set type location
    set internet-service-id 65536
    set country-id 840
    set region-id 283
    set city-id 23352
  next
end
```

2. View the IP ranges in the location-based internet service:

```
# diagnose internet-service id 65536 | grep "country(840) region(283) city(23352)"
```

3. Add the ISDB object to a policy:

```
config firewall policy
  edit 99
    set name "Demo_Policy"
    set srcintf "wan2"
    set dstintf "wan1"
    set srcaddr "all"
    set internet-service enable
    set internet-service-name "test-location-isdb-1"
    set action accept
    set schedule "always"
    set logtraffic all
    set logtraffic-start enable
```



```

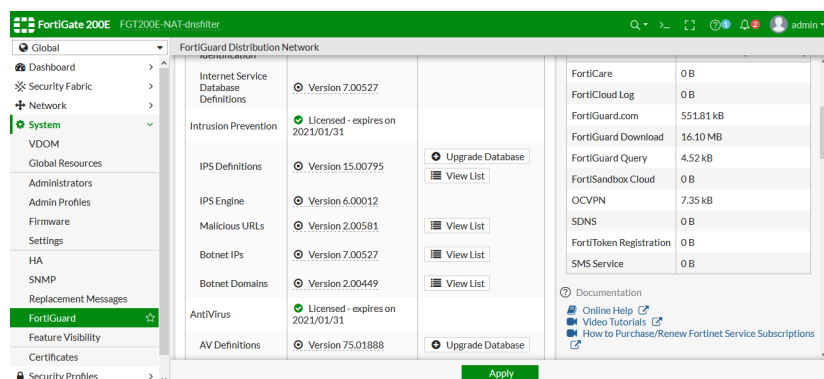
        set auto-asic-offload disable
        set comments "1"
        set nat enable
    next
end

```

## IP definitions database merged into the internet service database

The IP definitions database (IPDB, previously known as the IRDB) is merged into the internet service database (ISDB, also known as FFDB). Botnet C&C IP blocking now uses the ISDB as a source.

In the *License Information* table at *System > FortiGuard*, *Botnet IPs* and *Internet Service Database Definitions* have the same database version.



## Updating object versions

When updating object versions in the CLI, Botnet IPs is not listed. Internet-service Database Apps and Internet-service Database Maps are listed, and show the version for *Botnet IPs* and *Internet Service Database Definitions*.

```
# diagnose autoupdate version
```

```
.....
```

```
Internet-service Database Apps
```

```
-----
```

```
Version: 7.00528
```

```
Contract Expiry Date: n/a
```

```
Last Updated using scheduled update on Fri Mar 13 12:48:18 2020
```

```
Last Update Attempt: Fri Mar 13 16:48:10 2020
```

```
Result: No Updates
```

```
Internet-service Database Maps
```

```
-----
```

```
Version: 7.00528
```

```
Contract Expiry Date: n/a
```

```
Last Updated using scheduled update on Fri Mar 13 12:48:18 2020
```

```
Last Update Attempt: Fri Mar 13 16:48:10 2020
```

```
Result: No Updates
```

```
.....
```

## Update debug messages

In FortiOS 6.4 update debug messages, there is no query for the IBDB object:

6.4.0:

```
pack_obj[196]-Packing obj=Protocol=3.2|Command=Update|Firmware=FG200E-FW-6.04-
1565|SerialNumber=FG200E4Q17900126|UpdateMethod=0|AcceptDelta=1|DataItem=06004000APDB00105-
00015.00795-2003120019*06004000AVDB00201-00075.01892-2003131320*06004000AVDB00701-
00075.01892-2003131320*06004000MMDB00101-00075.01916-2003131321*06004000FLDB00201-
00075.01893-2003131325*06004000DBDB00100-00002.00450-2003131322*06004000NIDS02505-
00015.00795-2003120019*06004000ISDB00105-00000.00000-0101010000*06004000MUDB00103-
00002.00581-2003130417*06004000CIDB00000-00001.00096-
2003131527*06004000IPGO00000030492003122111*00000000FCNI00000-00000.00000-
0000000000*00000000FDNI00000-00000.00000-0000000000*01000000FSCI00100-00000.00000-
0000000000*06004000AVEN02800-00006.00144-2002220146*06004000FLEN06700-00006.00012-
2003110118*06004000FLEN05000-00001.00009-1906061402*06004000FFDB00307-00007.00528-
2003131142*06004000FFDB00407-00007.00528-2003131142*06004000UWDB00100-00002.00709-
2003131105*06004000CRDB00000-00001.00015-1907031016*06004000SFAS00000-00003.00000-
2002130915*06004000MCDB00100-00001.00254-2003091200*02000000FNSD00000-00000.00008-0000000000
```

6.2.3:

```
pack_obj[192]-Packing obj=Protocol=3.2|Command=Update|Firmware=FG200E-FW-6.02-
1093|SerialNumber=FG200E4Q17904482|UpdateMethod=0|AcceptDelta=1|DataItem=06002000APDB00104-
00015.00795-2003120019*06002000AVDB00201-00075.02861-2003120945*06002000MMDB00101-
00075.01920-2003131421*06002000IBDB00101-00004.00634-2003111709*06002000DBDB00100-
00002.00450-2003131322*06002000NIDS02504-00015.00795-2003120019*06002000ISDB00104-
00015.00795-2003120019*06002000MUDB00103-00002.00581-2003130417*06002000CIDB00000-
00001.00097-2003091749*06002000IPGO00000030492003122111*00000000FCNI00000-00000.00000-
0000000000*00000000FDNI00000-00000.00000-0000000000*01000000FSCI00100-00000.00000-
0000000000*06002000AVEN02800-00006.00144-2002220146*06002000FLEN07300-00005.00203-
2002242346*06002000FLEN05000-00001.00009-1906061402*06002000FFDB00306-00007.00528-
2003131137*06002000FFDB00406-00007.00528-2003131137*06002000UWDB00100-00002.00709-
2003131105*06002000CRDB00000-00001.00015-1907031016*06002000SFAS00000-00002.00033-
1911121935*06002000MCDB00100-0
```

## Diagnosing botnet IPs

Botnet IPs can be diagnosed with the following CLI command:

```
# diagnose sys botnet-ip {hit | list | find | flush}
```

Command	Description
hit	Show botnet IP entry hit count data.
list	List botnet IP entries.
find <ip> <port> <protocol>	Find botnet IP entries. Enter the IP address, port number, and protocol number to search the entries.
flush	Flush botnet IP entry hit count data.

## Extend ISDB to include well-known MAC address list

ISDB now includes well-known vendor MAC address range lists. The lists can only be used for source MAC addresses in IPv4 policies, and include the vendor name and the MAC address ranges that the vendor belongs to.

### To view the vendor list:

```
# diagnose vendor-mac id
Please input Vendor MAC ID.
ID: 1 name: "Asus"
ID: 2 name: "Acer"
ID: 3 name: "Amazon"
ID: 4 name: "Apple"
ID: 5 name: "Xiaomi"
ID: 6 name: "BlackBerry"
ID: 7 name: "Canon"
ID: 8 name: "Cisco"
ID: 9 name: "Linksys"
ID: 10 name: "D-Link"
ID: 11 name: "Dell"
ID: 12 name: "Ericsson"
ID: 13 name: "LG"
ID: 14 name: "Fujitsu"
ID: 15 name: "Fitbit"
ID: 16 name: "Fortinet"
ID: 17 name: "OPPO"
ID: 18 name: "Hitachi"
ID: 19 name: "HTC"
ID: 20 name: "Huawei"
ID: 21 name: "HP"
ID: 22 name: "IBM"
ID: 23 name: "Juniper"
ID: 24 name: "Lenovo"
ID: 25 name: "Microsoft"
ID: 26 name: "Motorola"
ID: 27 name: "Netgear"
ID: 28 name: "Nokia"
ID: 29 name: "Nintendo"
ID: 30 name: "PaloAltoNetworks"
ID: 31 name: "Polycom"
ID: 32 name: "Samsung"
ID: 33 name: "Sharp"
ID: 34 name: "Sony"
ID: 35 name: "Toshiba"
ID: 36 name: "VMware"
ID: 37 name: "Vivo"
ID: 38 name: "Zyxel"
ID: 39 name: "ZTE"
```

### To view the MAC address ranges for a vendor:

```
# diagnose vendor-mac id 16
Vendor MAC: 16(Fortinet)
Version: 0000700021
Timestamp: 201908081432
```

```
Number of MAC ranges: 6
00:09:0f:00:00:00 - 00:09:0f:ff:ff:ff
04:d5:90:00:00:00 - 04:d5:90:ff:ff:ff
08:5b:0e:00:00:00 - 08:5b:0e:ff:ff:ff
70:4c:a5:00:00:00 - 70:4c:a5:ff:ff:ff
90:6c:ac:00:00:00 - 90:6c:ac:ff:ff:ff
e8:1c:ba:00:00:00 - e8:1c:ba:ff:ff:ff
```

**To query the vendor of a specific MAC address or range:**

```
# diagnose vendor-mac match 00:09:0f:ff:ff:ff 48
Vendor MAC: 16(Fortinet), matched num: 1
```

**To use the vendor ID in a firewall policy:**

```
config firewall policy
  edit 9
    set name "policy_id_9"
    set srcintf "wan2"
    set dstintf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set src-vendor-mac 36 16
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set auto-asic-offload disable
    set nat enable
  next
end
```

Only packets whose source MAC address belong to Fortinet or VMware are passed by the policy.

## GeoIP matching by registered and physical location

IP addresses have both a physical and registered location in the geography IP database. Sometimes these two locations are different. The new `geoip-match` command allows users to match an IP address in an IPv4 policy to its physical or registered location when a GeoIP is used as a source or destination address.

In the following example, the physical location of 220.243.219.10 is CA (Canada), the registered location is CN (China), and it is not an anycast IP.

**To configure GeoIP matching based on registered location:**

1. Create a firewall policy to match the IP:

```
config firewall policy
  edit 1
    set name "policy_id_1"
    set srcintf "wan2"
    set dstintf "wan1"
    set srcaddr "all"
    set dstaddr "test-geoip-CN"
```

```

        set action accept
        set schedule "always"
        set service "ALL"
        set geoip-match registered-location
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end

```

Since CA is applied as a destination address and registered location IP matching is enabled, if the destination IP of the traffic is 220.243.219.10, then the traffic will be blocked because the registered location is CN.

**2. Verify that the policy is blocking traffic from the IP address:**

```

# diagnose sniffer packet any icmp 4
interfaces=[any]
filters=[icmp]
5.383798 wan2 in 10.1.100.41 -> 220.243.219.10: icmp: echo request
6.381982 wan2 in 10.1.100.41 -> 220.243.219.10: icmp: echo request
7.382608 wan2 in 10.1.100.41 -> 220.243.219.10: icmp: echo request
^C
3 packets received by filter
0 packets dropped by kernel

```

**To configure GeoIP matching based on physical location:**

**1. Create a firewall policy to match the IP:**

```

config firewall policy
    edit 1
        set name "policy_id_1"
        set srcintf "wan2"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "test-geoip-CA"
        set action accept
        set schedule "always"
        set service "ALL"
        set geoip-match physical-location
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end

```

Since CA is applied as a destination address and physical location IP matching is enabled, if the destination IP of the traffic is 220.243.219.10, then the traffic will pass through.

**2. Verify that the policy is allowing traffic from the IP address:**

```

# diagnose sniffer packet any icmp 4
interfaces=[any]
filters=[icmp]
5.273985 wan2 in 10.1.100.41 -> 220.243.219.10: icmp: echo request
5.274176 wan1 out 172.16.200.10 -> 220.243.219.10: icmp: echo request
6.274426 wan2 in 10.1.100.41 -> 220.243.219.10: icmp: echo request
6.274438 wan1 out 172.16.200.10 -> 220.243.219.10: icmp: echo request
7.273978 wan2 in 10.1.100.41 -> 220.243.219.10: icmp: echo request

```

```
7.273987 wan1 out 172.16.200.10 -> 220.243.219.10: icmp: echo request
^C
6 packets received by filter
0 packets dropped by kernel
```

## Group address objects synchronized from FortiManager

Address objects from external connectors that are learned by FortiManager are synchronized to FortiGate. These objects can be grouped together with the FortiGate CLI to simplify selecting connector objects in the FortiGate GUI. Multiple groups can be created.

This option is only available for objects that are synchronized from FortiManager.

### To add an object to a connector group:

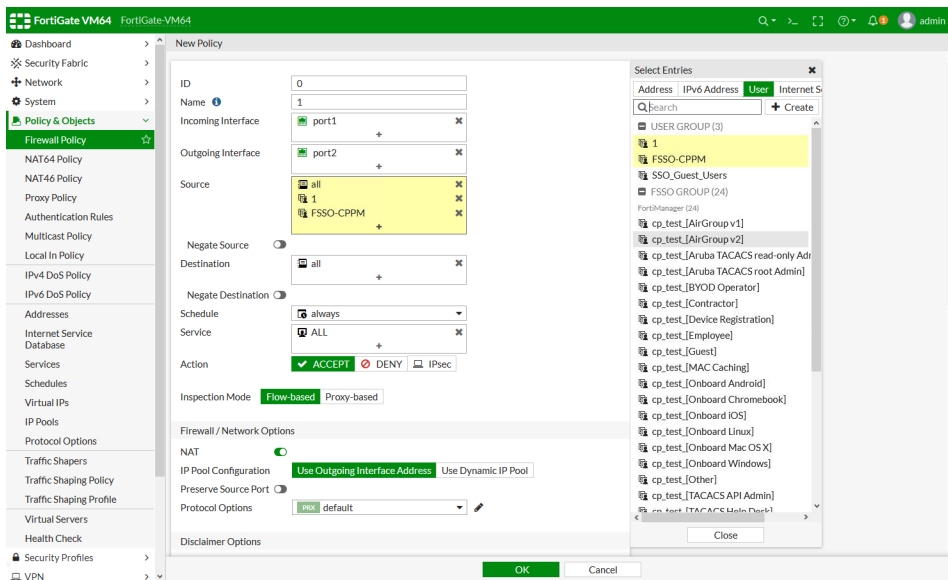
```
config user adgrp
  edit <object_name>
    set server-name "FortiManager"
    set connector-source <group_name>
  next
end
```

## Example

In this example, objects learned by the FortiManager from an Aruba ClearPass device are synchronized to the FortiGate. Some of the objects are then added to a group called *ClearPass* to make them easier to find in the object list when creating a firewall policy.



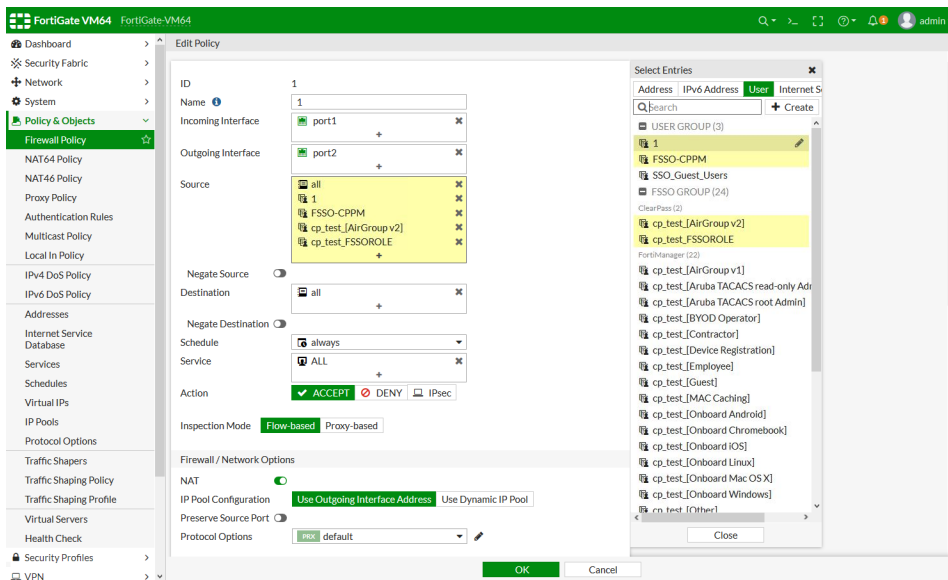
Prior to being grouped, the synchronized objects are listed under the FortiManager heading in the object lists.



To add some of the objects to a group:

```
config user adgrp
    edit "cp_test_FSSOROLE"
        set server-name "FortiManager"
        set connector-source "ClearPass"
    next
    edit "cp_test_[AirGroup v2]"
        set server-name "FortiManager"
        set connector-source "ClearPass"
    next
end
```

The objects are now listed under the *ClearPass* heading.



## Increase in maximum number of VIP real servers

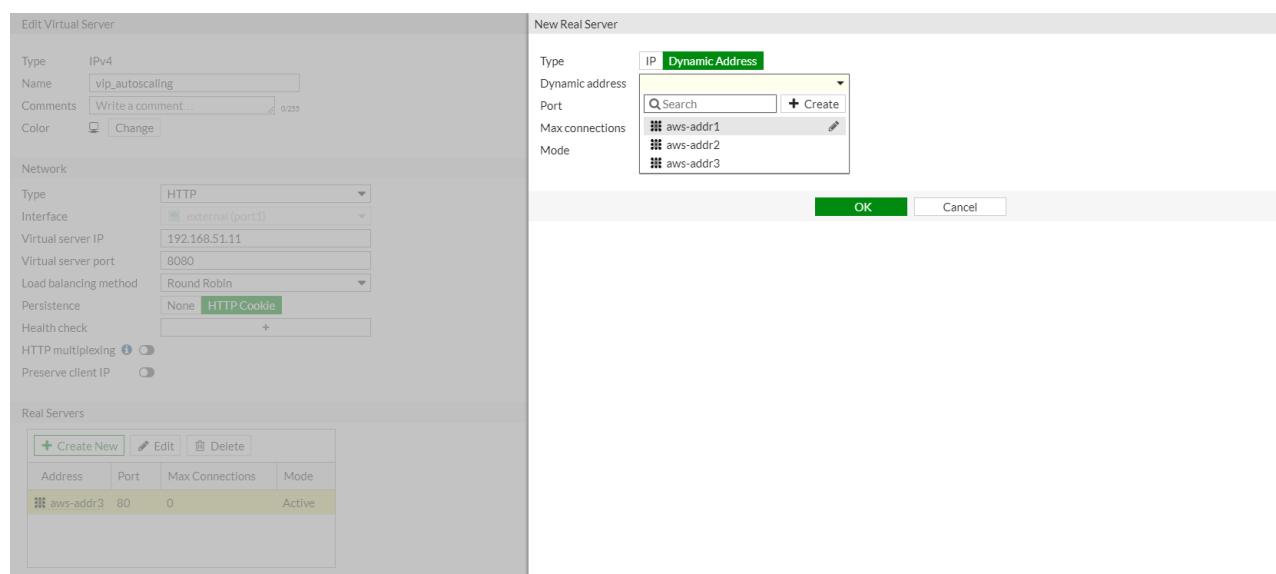
Except for desktop models, all other platforms' table size of VIP real servers have increased as follows:

- 1U platforms increased from 8 to 16
- 2U platforms increased from 32 to 64
- High-end platforms increased from 32 to 256

## GUI support for real server configurations using address objects - 6.4.2

Dynamic address objects can be configured as real servers in the GUI.

When creating a new real server (*Policy & Objects > Virtual Servers*), users can select either *IP* or *Dynamic Address* as the *Type*:



Dynamic addresses are visible in the *Real Servers* list. Hover over an address to view more information:



Edit Virtual Server

Type
IPv4

Name
vip\_autoscaling

Comments
Write a comment...
0/255

Color
Change

Network

Type
HTTP

Interface
external (port1)

Virtual server IP
192.168.51.11

Virtual server port
8080

Load balancing

Address
aws-addr3

Persistence

Type
Dynamic

Health check

Sub Type
Fabric Connector Address

HTTP multiple

SDN Connector
aws-sdn

Preserve client

Filter
Tag.Name=AZHA-Ubuntu-net52-pri-192.168.52.0 | Tag.Name=AZHA-Ubuntu-net62-pri-192.168.62.0

Real Servers

+ Create

Address
Edit

aws-addr3
80
0
Active

OK

Cancel

# Security profiles

This section includes information about security profile related new features:

- [Antivirus on page 292](#)
- [Application control on page 300](#)
- [Web filter on page 306](#)
- [IPS on page 316](#)
- [Others on page 320](#)

## Antivirus

This section includes information about antivirus related new features:

- [Security Profiles enhancements on page 292](#)
- [Antivirus uses the extended database by default on page 298](#)
- [Scan compressed messages over CIFS protocol in proxy mode 6.4.2 on page 299](#)

## Security Profiles enhancements

### Feature set option

To more clearly show the features specific to proxy-based mode, use the new *Feature set* option to select *Flow-based* or *Proxy-based*. When you select *Flow-based* or *Proxy-based*, only the features for that mode are available.

The following pages have the *Feature set* option:

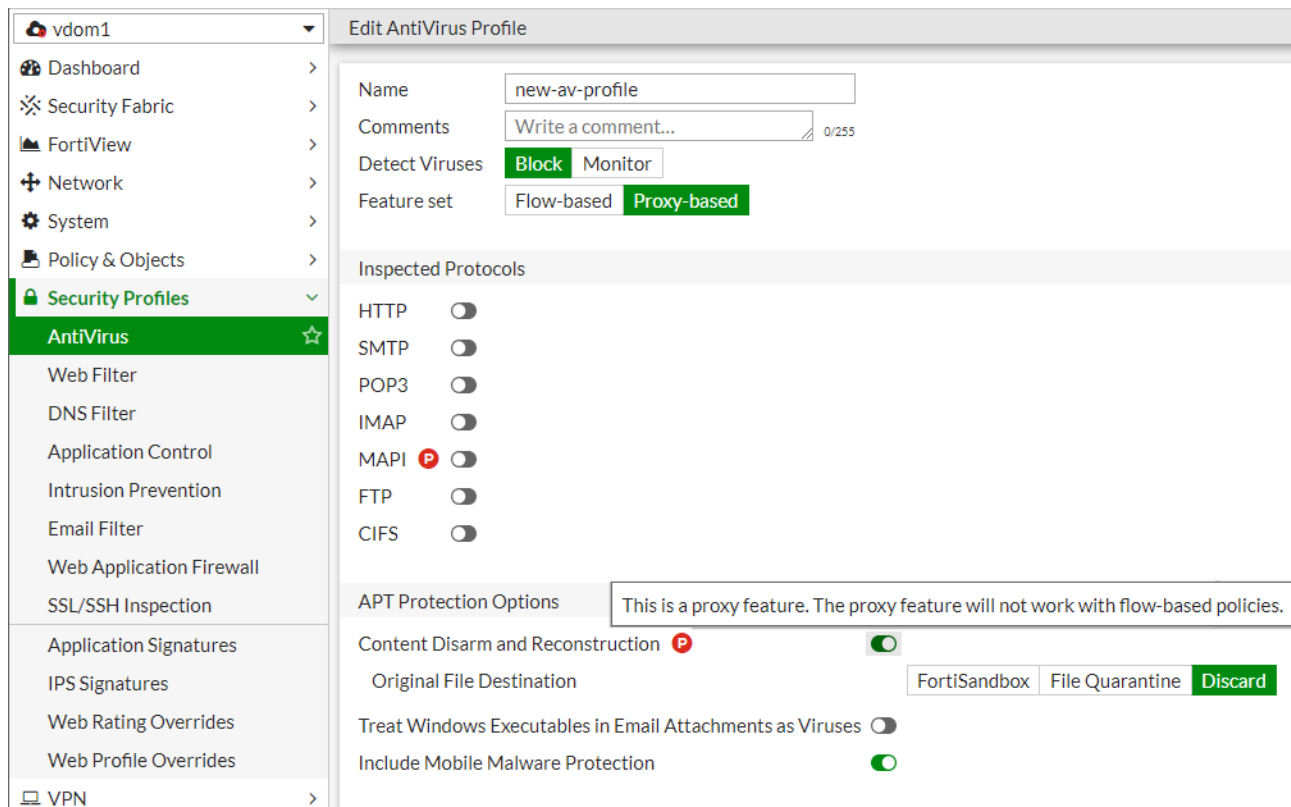
- *Security Profiles > AntiVirus*
- *Security Profiles > Web Filter*
- *Security Profiles > Email Filter*
- *Security Profiles > Data Leak (CLI only)*
- *Policy & Objects > Protocol Options*

Example of the *Feature set* option in *Security Profiles > AntiVirus*:

The screenshot shows the 'Edit AntiVirus Profile' configuration page. On the left is a sidebar with a tree view under 'Security Profiles'. 'AntiVirus' is selected and highlighted in green. Other options in the sidebar include Web Filter, DNS Filter, Application Control, Intrusion Prevention, SSL/SSH Inspection, Application Signatures, IPS Signatures, Web Rating Overrides, Web Profile Overrides, VPN, User & Device, and Wi-Fi Switch. The main content area is titled 'Edit AntiVirus Profile'. It contains several fields: 'Name' (default), 'Comments' (Scan files and block viruses.), 'Detect Viruses' (Block and Monitor buttons), and 'Feature set' (Flow-based and Proxy-based buttons). The 'Feature set' section is enclosed in a red rectangular box. Below this is the 'Inspected Protocols' section, which lists HTTP, SMTP, POP3, IMAP, FTP, and CIFS, each with a toggle switch. The first five are turned on, and CIFS is turned off.

Edit AntiVirus Profile	
Name	default
Comments	Scan files and block viruses. 29/255
Detect Viruses	<input checked="" type="button" value="Block"/> <input type="button" value="Monitor"/>
Feature set	<input checked="" type="button" value="Flow-based"/> <input type="button" value="Proxy-based"/>
Inspected Protocols	
HTTP	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>
FTP	<input checked="" type="checkbox"/>
CIFS	<input type="checkbox"/>

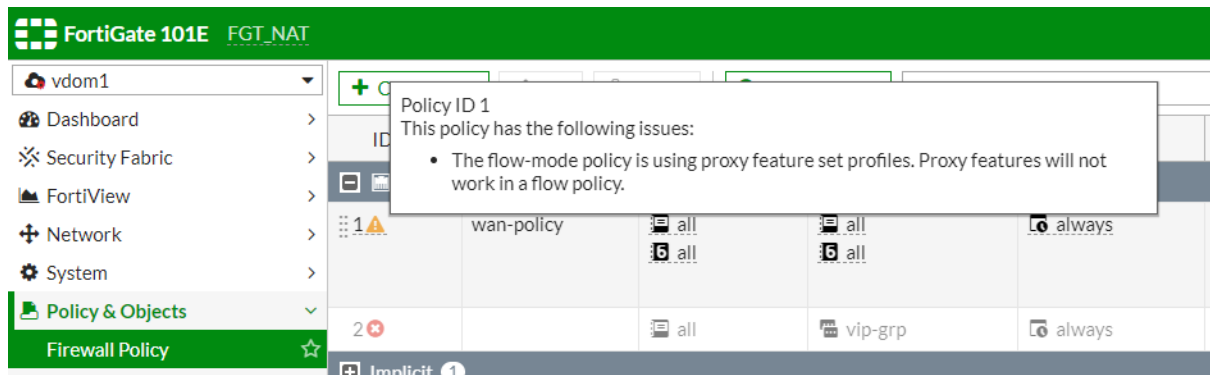
If you select *Proxy-based*, a red P icon indicates the proxy-only features. FortiOS.



When you configure firewall policies:

- If the inspection mode is flow-based, dropdown menus only display profiles with flow-based feature sets.
- If the inspection mode is proxy-based, dropdown menus display profiles with flow-based or proxy-based feature sets.

If a flow-based inspection policy has a proxy-based profile assigned, a warning icon and tooltip informs you that proxy features do not work in a flow-based policy. This warning also appears when you use the CLI to assign security profiles.



## Upgrade support

Upgrading from 6.2.x to 6.4.0 causes the following changes to security profiles.

Upgrade scenario	Result after upgrade
Profile was assigned exclusively to flow-base firewall policies in 6.2.x.	feature-set = flow
Profile was assigned exclusively to proxy-base firewall policies in 6.2.x.	feature-set = proxy
Profile was assigned to both flow-base and proxy-base firewall policies in 6.2.x.	feature-set = proxy
Profile was not assigned to any firewall policies in 6.2.x.	feature-set = flow

## Configure security profiles using CLI

**To configure the Antivirus security profile using the CLI:**

```
config antivirus profile
  edit new-av-profile
    set comment <string>
    set feature-set {flow | proxy}
    set ftgd-analytics {disable | suspicious | everything}
    ...
  next
end
```

See [Configure Antivirus profiles](#) in the FortiOS CLI Reference for more information.

**To configure the Web Filter security profile using the CLI:**

```
config webfilter profile
  edit "new-wf-profile"
    set comment <string>
    set feature-set {flow | proxy}
    ...
    config ftgd-wf
      unset options
      config filters
      ...
    end
  end
next
end
```

See [Configure Web filter profiles](#) in the FortiOS CLI Reference for more information.

**To configure the Email Filter security profile using the CLI:**

```
config emailfilter profile
  edit "new-ef-profile"
    set comment <string>
    set feature-set {flow | proxy}
    ...
```

```
    next
end
```

See [Configure Email filter profiles](#) in the FortiOS CLI Reference for more information.

### To configure the DLP security profile using the CLI:

```
config dlp sensor
    edit "new-dlp-profile"
        set comment <string>
        set feature-set {flow | proxy}
        ...
    next
end
```

See [Configure DLP sensors](#) in the FortiOS CLI Reference for more information.

### To configure Protocol Options in Policy & Objects using the CLI:

```
config firewall profile-protocol-options
    edit "new-protocol-options"
        set feature-set {flow | proxy}
        config http
            set ports 80
            unset options
            unset post-lang
        end
        config ftp
            set ports 21
            set options splice
        end
        config imap
            set ports 143
            set options fragmail
        end
        ...
    next
end
```

See [Configure protocol options](#) in the FortiOS CLI Reference for more information.

## Antivirus profiles use hybrid scanning as default

In flow-based Antivirus profiles, the scan-mode option is removed. Flow-based Antivirus profiles use the default hybrid scanning method to process traffic. Legacy mode is available for diagnostics only.



When upgrading from 6.2.x to 6.4.0, Antivirus profiles assigned to flow-based firewall policies only operate in the default hybrid mode regardless of the previous scan-mode setting.

---

In CLI, `scan-mode` options are only available for proxy-based Antivirus profiles. The `scan-mode` options are not available for flow-based Antivirus profiles.

```
config antivirus profile
  edit "new-av-profile"
    set comment ''
    set replacemsg-group ''
    set feature-set proxy
    set mobile-malware-db enable
    config http
      unset options
      unset archive-block
      unset archive-log
      set emulator enable
      set outbreak-prevention disabled
    end
    ...
    set av-virus-log enable
    set av-block-log enable
    set extended-log disable
    set scan-mode default
  next
end
```

set ?	
comment	Comment.
replacemsg-group	Replacement message group customized for this profile.
feature-set	Flow/proxy feature set.
mobile-malware-db	Enable/disable using the mobile malware signature database.
av-virus-log	Enable/disable AntiVirus logging.
av-block-log	Enable/disable logging for AntiVirus file blocking.
extended-log	Enable/disable extended logging for antivirus.
<b>scan-mode</b>	<b>Choose between default scan mode and legacy scan mode.</b>

## Diagnostics

The following diagnostic commands are meant for troubleshooting only.

```
diagnose ips av mode ?
  hybrid  Enable/disable hybrid scan mode.
  show    Show status of hybrid scan mode.
```

### To check flow-base AV scan mode status:

```
diagnose ips av mode show
  Flow-av hybrid scan: Enabled
  Flow-av hybrid scan: Enabled
  Flow-av hybrid scan: Enabled
  Flow-av hybrid scan: Enabled
```

### To disable hybrid scan for flow-base AV and enable full scan:



This command does not persist over a reboot. Flow-av hybrid scan is enabled by default.

---

```
diagnose ips av mode hybrid disable
```

```
diagnose ips av mode show
  Flow-av hybrid scan: Disabled
  Flow-av hybrid scan: Disabled
  Flow-av hybrid scan: Disabled
  Flow-av hybrid scan: Disabled
```

**To enable hybrid scan for flow-based AV and disable full scan to go back to default:**

```
diagnose ips av mode hybrid enable
```

```
diagnose ips av mode show
  Flow-av hybrid scan: Enabled
  Flow-av hybrid scan: Enabled
  Flow-av hybrid scan: Enabled
  Flow-av hybrid scan: Enabled
```

## Antivirus uses the extended database by default

Starting with this version, the FortiGate uses the extended database as its default antivirus database. The normal database option is no longer supported. On FortiGate models that support the extreme database, you have the option to choose either the extended or extreme database. The FortiGate 300D is the lowest model that supports the extreme database. All VMs support the extreme database.

Under `config antivirus settings`, the `default-db` parameter has been removed.

FortiGate models that support extreme set database have a new `use-extreme-db` parameter.

By default, `use-extreme-db` is disabled so the FortiGate uses its normal and extended set databases. When you enable `use-extreme-db`, the FortiGate uses the extreme set database.

## Upgrade support

Upgrading from 6.2.x to 6.4.0 causes the following changes.

Before upgrade	After upgrade
default-db = normal	use-extreme-db = disable (hidden on low-end models)
default-db = extended	use-extreme-db = disable (hidden on low-end models)
default-db = extreme	use-extreme-db = enable

## Antivirus settings in the CLI

On low-end models, `use-extreme-db` is hidden. This example shows the CLI output from a FortiGate 101E.

```
# show full-configuration antivirus settings
config antivirus settings
  set grayware enable
  set override-timeout 0
end
```



**To configure the extreme database on a high-end model:**

```
config antivirus settings
    set use-extreme-db enable
    set grayware enable
    set override-timeout 0
end
```



This example shows the CLI output from a FortiGate 600D.

## Scan compressed messages over CIFS protocol in proxy mode - 6.4.2

With the newly added compression methods in the CIFS protocol, FortiGates can scan these compressed messages in proxy mode. The following compression algorithms are supported:

- LZNT1
- LZ77
- LZ77+Huffman

This feature is supported on Windows 10 and Windows Server 2019 with update version 1809 and later.

The following example uses Ubuntu 20.04 as an SMB client and Windows 10 as an SMB server. A Python script is used on the client for message compression.

**To scan messages using the CIFS protocol in proxy mode:**

1. Create a file filter profile using proxy mode for CIFS and apply it to a policy (see [File filter](#) for more information). Traffic is blocked by the file filter in this example:

```
root@pc06:~/qa/tools/smb_tests# python3 data_path_tests.py --server-ip 172.16.200.150 --port 445 --username "win10-pro\ssh_user" --password 123456 --share shares --
encrypt 0 --compress 1 --data-tuple data_tuples_doc.txt

Processing data tuple of key 'data4' and value
{'connection_id': 0, 'session_id': 0, 'tree_id': 0, 'compound': 0, 'type': 1, 'file_path': './sample', 'file_name': 'test.doc', 'range': 'none', 'result': 0}

Reading actual file
file test.doc is read with size 19456
File test.doc is not sent as expected with error The exception is (<class 'smbprotocol.exceptions.SMBResponseException'>, SMBResponseException(<smbprotocol.connecti
on.SMB2HeaderResponse object at 0x7ffb2d37e430>, 3221225506), <traceback object at 0x7ffb2d3aa340>).
```

2. Verify that the WAD recognizes the compressed message:

```
# diagnose wad debug enable level verbose
# diagnose wad debug enable category cifs
cifs_nbss_identify_protocol(583): nbss detected encapsulated compressed smb3 message
smb2_nbss_alloc(1108): smb2 nbss 0x7ff471b0a1a0 allocated
smb2_parse_stream(5337): smb2 parsing 118 plain-text bytes
smb2_parsing_alloc(1551): smb2 parsing 0x7ff4709fbc0 allocated
smb2_payload_alloc(1025): smb2 payload 0x7ff470678e00 allocated
smb2_msg_alloc(1612): smb2 message 0x7ff471aadd70 allocated
smb2_hdr_print(1707): smb2 CON Request [mid 3, sid 35184372088853, tid 0, st 0, r 0]
smb2_parse_message(5249): smb2 processing 118 message bytes
```

3. Verify the UTM log:

```
1: date=2020-07-08 time=16:10:26 logid="1900064000" type="utm" subtype="file-filter"
eventtype="file-filter" level="warning" vd="root" eventtime=1594249826958143704 tz="-
```

```
0700" policyid=1 sessionid=18382 srcip=10.1.100.66 srcport=58004 srcintf="port21"
srcintfrole="undefined" dstip=172.16.200.150 dstport=445 dstintf="port23"
dstintfrole="undefined" proto=6 service="CIFS" profile="filefilter" direction="outgoing"
action="blocked" filtername="1" filename="test.doc" filesize=19456 filetype="msoffice"
msg="File was blocked by file filter."
```

4. Use Python for CIFS traffic with different compression algorithms. The compressed message and compression algorithm is visible in the packet capture.

- LZNT1:

22	16:02:51.811604	10.1.100.66	172.16.200.150
23	16:02:51.811609	172.16.200.150	10.1.100.66

```

> Internet Protocol Version 4, Src: 10.1.100.66, Dst: 172.16.200.150
> Transmission Control Protocol, Src Port: 57994, Dst Port: 445, Seq: 922, Ack: 1075, Len: 185
> NetBIOS Session Service
> SMB2 (Server Message Block Protocol version 2)
  SMB2 Compression Transform Header
  ProtocolId: 0xfc534d42
  OriginalSize: 240
  CompressionAlgorithm: LZNT1 (0x0001)
  Reserved: 0000
  Offset: 0x00000000
  Compressed SMB3 data

```

- LZ77:

22	16:04:45.672079	10.1.100.66	172.16.200.150
23	16:04:45.672079	172.16.200.150	10.1.100.66

```

> Internet Protocol Version 4, Src: 10.1.100.66, Dst: 172.16.200.150
> Transmission Control Protocol, Src Port: 57996, Dst Port: 445, Seq: 923, Ack: 1075, Len: 185
> NetBIOS Session Service
> SMB2 (Server Message Block Protocol version 2)
  SMB2 Compression Transform Header
  ProtocolId: 0xfc534d42
  OriginalSize: 240
  CompressionAlgorithm: LZ77 (0x0002)
  Reserved: 0000
  Offset: 0x00000000
  Compressed SMB3 data

```

- LZ77+Huffman:

25	16:06:09.866518	10.1.100.66	172.16.200.150
26	16:06:09.866634	172.16.200.150	10.1.100.66

```

> Transmission Control Protocol, Src Port: 57998, Dst Port: 445, Seq: 2616, Ack: 1263, Len: 297
> [2 Reassembled TCP Segments (1745 bytes): #20(1448), #21(297)]
> NetBIOS Session Service
> SMB2 (Server Message Block Protocol version 2)
  SMB2 Compression Transform Header
  ProtocolId: 0xfc534d42
  OriginalSize: 19568
  CompressionAlgorithm: LZ77+Huffman (0x0003)
  Reserved: 0000
  Offset: 0x00000000
  Compressed SMB3 data

```

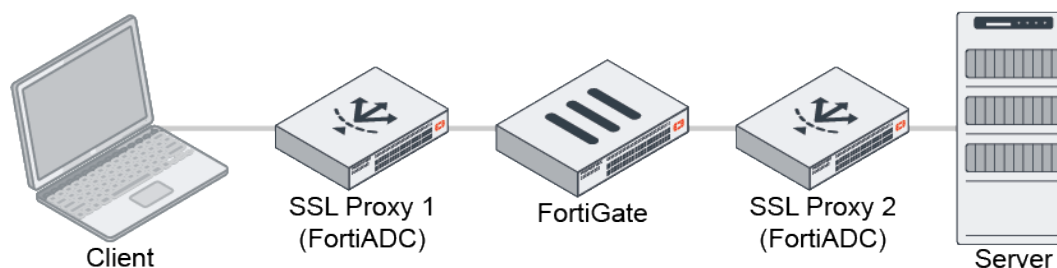
## Application control

This section includes information about application control related new features:

- [SSL-based application detection over decrypted traffic in a sandwich topology on page 301](#)
- [Matching multiple parameters on application control signatures on page 301](#)
- [Allow exclusion of signatures in application control profile 6.4.3 on page 304](#)

## SSL-based application detection over decrypted traffic in a sandwich topology

When a FortiGate is sandwiched between SSL encryption and decryption devices, the FortiGate can process the decrypted traffic that passes between those devices. This feature adds support for decrypted traffic in application control. In some pre-defined signatures, the signature is pre-marked with the `require_ssl_di` tag. The `force-inclusion-ssl-di-sigs` option under `application list` allows users to control the inspection of dissected traffic. When this option is enabled, the IPS engine forces the pre-marked SSL-based signatures to be applied to the decrypted traffic of the respective applications. In the following topology, SSL Proxy 1 handles the client connection and SSL Proxy 2 handles the server connection, leaving the content unencrypted as traffic passes through the FortiGate.



### To configure SSL-based application detection over decrypted traffic:

```

config application list
  edit "test"
    set force-inclusion-ssl-di-sigs {enable | disable}
  next
end
  
```

### Example pre-marked SSL-based signature:

```

F-SBID( --vuln_id 15722; --attack_id 42985; --name "Facebook_Chat"; --group im; --protocol tcp; --default_action pass; -
-revision 4446; --app_cat 23; --vendor 3; --technology 1; --behavior 9; --pop 4; --risk 2; --language "Multiple"; --weight 20;
--depend-on 15832; --depend-on 38468; --require_ssl_di "Yes"; --casi 1; --casi 8; --parent 15832; --app_port
"TCP/443"; --severity info; --status hidden; --service http; --flow from_client; --pattern "/pull?"; --context uri; --no_case; --
pattern ".facebook.com"; --context host; --no_case; --tag set, Tag.Facebook.Pull; --tag quiet; --scan-range 10m,all; --date
20190301;)
  
```



All signatures that include the `require_ssl_di` tag are pre-defined and cannot be customized.

## Matching multiple parameters on application control signatures

Application control signatures that support parameters (such as SCADA protocols) can have multiple parameters grouped together and matched at the same time. Multiple application parameter groups can be added to an override.

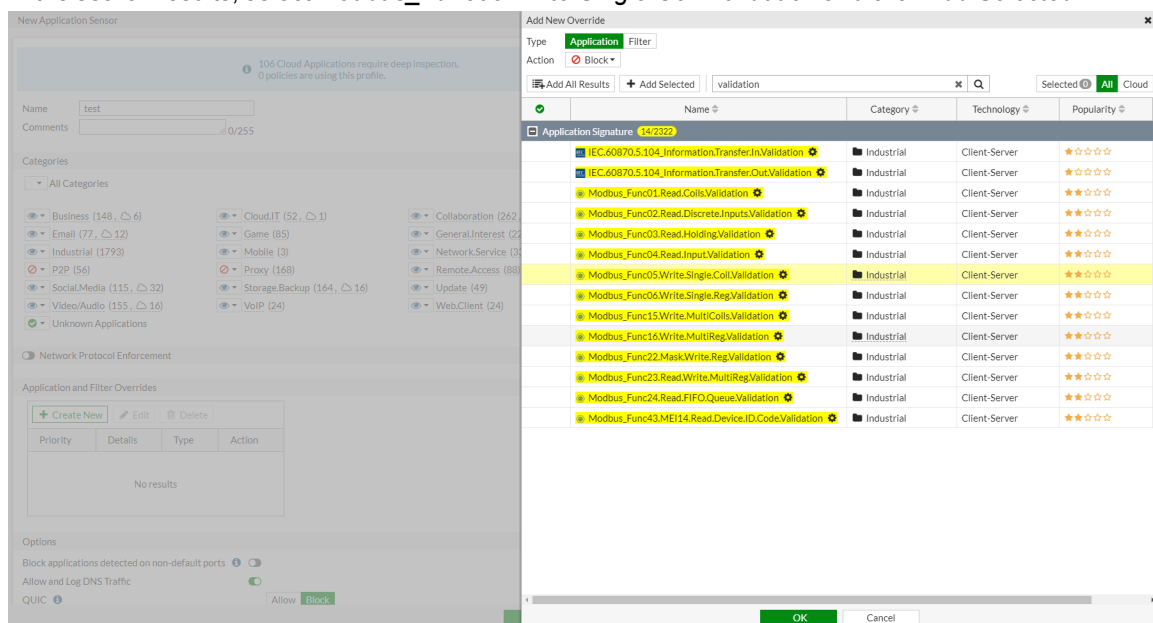
Traffic will be flagged if it matches at least one parameter group.

This example uses the `Modbus_Func05.Write.Single.Coil.Validation` signature. This is an industrial signature, so ensure that no signatures are excluded:

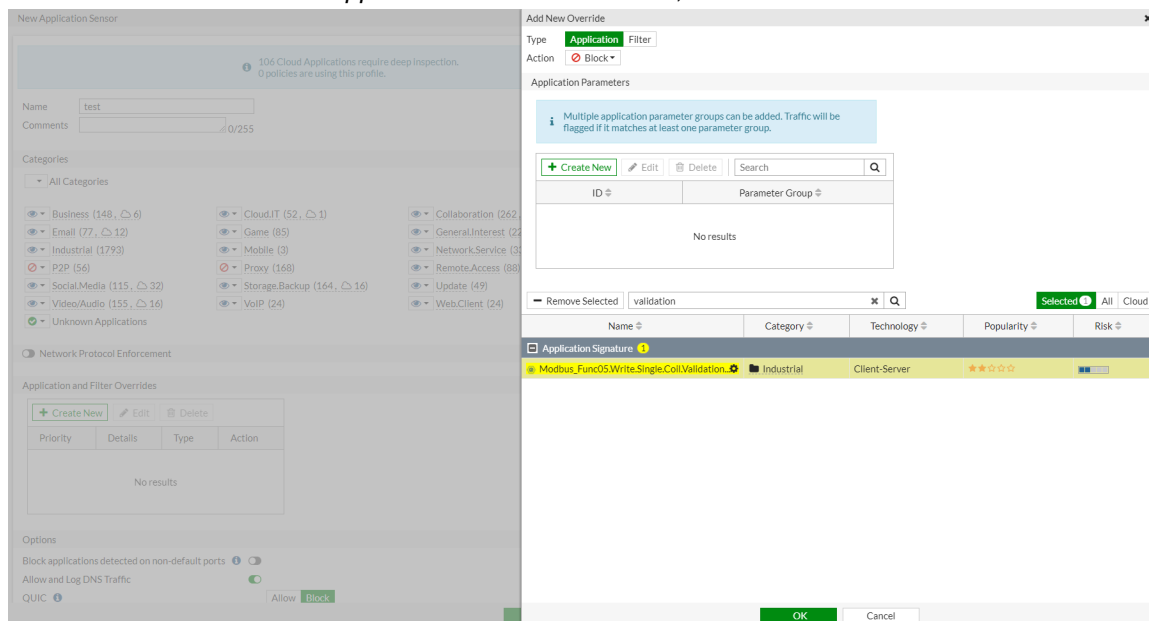
```
config ips global
    set exclude-signatures none
end
```

### To configure an application sensor with multiple parameters in the GUI:

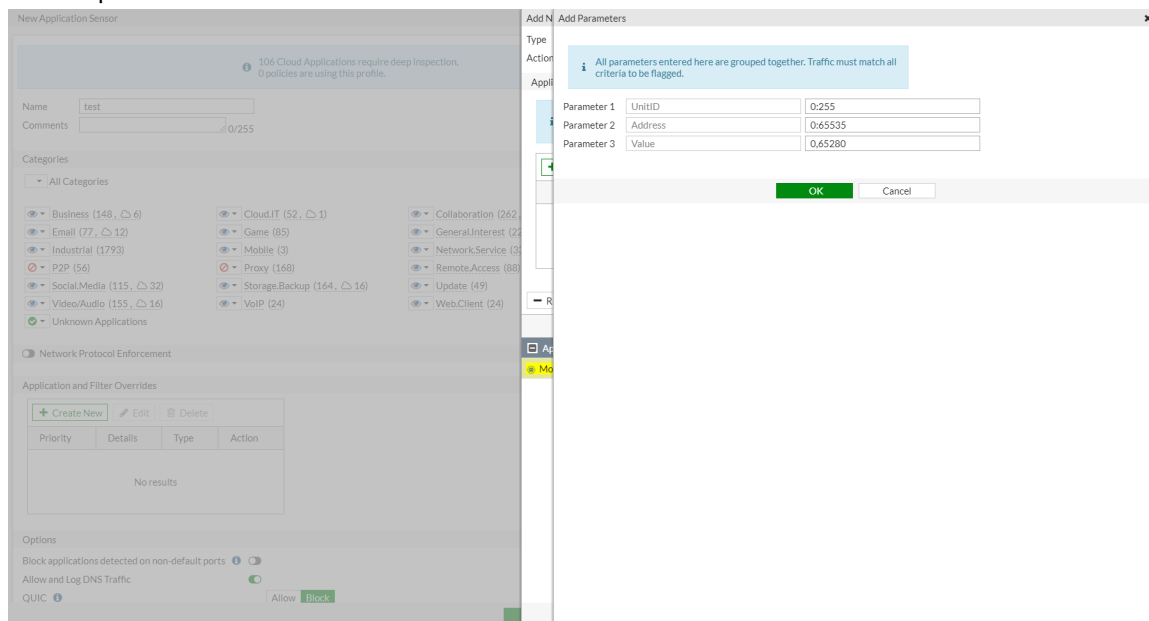
1. Go to **Security Profiles > Application Control** and click **Create New**, or edit an existing sensor.
2. In the **Application and Filter Overrides** table, click **Create New**.
3. Search for `Modbus_Func05.Write.Single.Coil.Validation` and press **Enter**. A gear icon beside the signature name indicates it has configurable application parameters.
4. In the search results, select `Modbus_Func05.Write.Single.Coil.Validation` and click **Add Selected**.



5. Click the **Selected** tab. In the **Application Parameters** section, click **Create New**.



6. Edit the parameter values as needed.



7. Click **OK**.  
 8. Add more signatures if needed.  
 9. Click **OK**.

### To configure an application sensor with multiple parameters in the CLI:

```
config application list
edit "test"
set other-application-log enable
config entries
edit 1
```

```
set application 48885
config parameters
  edit 1
    config members
      edit 1
        set name "UnitID"
        set value "0:255"
      next
      edit 2
        set name "Address"
        set value "0:65535"
      next
      edit 3
        set name "Value"
        set value "0,65280"
      next
    end
  next
end
next
edit 2
  set category 2 6
next
end
next
end
```

## Allow exclusion of signatures in application control profile - 6.4.3

In an application control list, the exclusion option allows users to specify a list of applications they wish to exclude from an entry filtered by category, technology, or others. By excluding the signature, the application is no longer processed on the entry in which it is excluded, but may match subsequent entries that exist.

### To configure signature exclusion:

```
config application list
  edit <name>
    config entries
      edit <id>
        set category <id>
        set exclusion {category technology ...}
        set action {pass | block | reset}
      next
    end
  next
end
```

## Examples

In the following example, category 23 (social media) is blocked in the entries, and signature 34527 (Instagram) is excluded from this entry. Traffic to Instagram will pass because the signature is removed from entry 1 and the action of other-application-action is set to pass.

**To configure signature exclusion:**

```
config application list
  edit "test"
    set other-application-action pass
    set unknown-application-action pass
    set other-application-log enable
    set unknown-application-log enable
    config entries
      edit 1
        set category 23
        set exclusion 34527
        set action block
      next
    end
  next
end
```

In the following example, entry 1 is configured so that category 23 (social media) is set to pass and signature 34527 (Instagram) is excluded. In entry 2, application 34527 (Instagram) is blocked, so the traffic to Instagram will be blocked, even though it is excluded in entry 1. Traffic to other signatures in category 23, such as Facebook, will still pass.

**To configure signature exclusion:**

```
config application list
  edit "test"
    set other-application-action pass
    set unknown-application-action pass
    set other-application-log enable
    set unknown-application-log enable
    config entries
      edit 1
        set category 23
        set exclusion 34527
        set action pass
      next
      edit 2
        set application 34527
        set action block
      next
    end
  next
end
```

In the following example, an explicit proxy is behind the FortiGate with an excluded signature for 107347980 (Proxy.HTTP) and category 6 (proxy) is set to block. The client will allow normal proxy traffic to pass, but it will discard all proxy application traffic (such as KProxy, Tor, and so on).

**To configure signature exclusion:**

```
config application list
  edit "test"
    set other-application-action pass
    set unknown-application-action pass
    set other-application-log enable
    set unknown-application-log enable
```

```
config entries
  edit 1
    set category 6
    set exclusion 107347980
    set action block
  next
end
next
end
```

## Web filter

This section includes information about web filter related new features:

- [Credential phishing prevention on page 306](#)
- [Explicitly enable custom categories for web filter profiles, SSL/SSH inspection profiles, and proxy addresses 6.4.2 on page 308](#)
- [Configure web filter profiles in NGFW policy mode 6.4.2 on page 312](#)
- [Remove the option to rate images by URL in Web filter profiles 6.4.3 on page 315](#)
- [Rating submission link on web filter block and warning pages 6.4.5 on page 315](#)

## Credential phishing prevention

When credential phishing prevention is enabled, the FortiGate scans for corporate credentials submitted to external websites and compares them to sensitive credentials stored in the corporate domain controller. Based on the configured antiphishing rules in proxy mode web filter profiles, the FortiGate will block the URL or alert the user if the credentials match ones that are stored on the corporate domain controller.

- The corporate domain controller must be configured on the credential-store. Credentials are matched based on sAMAccountName. UPN format is not currently supported.
- The antiphishing profile defines the corporate domain controller, antiphishing check option, default action if no rules match, antiphishing status, and so on.
- Inspection entries in the profile define what action occurs when the submission request matches the specified FortiGuard categories.
- The profile scans for pre-defined and custom username and password fields in the HTTP request, such as `username`, `auth`, and `password`. You can evaluate custom fields by configuring custom patterns.
- The URL filter defines individual URLs that the antiphish action (block or log) is applied to when the URL submission request matches.



Web-based URL filter actions and FortiGuard category-based filtering have higher priority than antiphishing URL filter actions and FortiGuard filtering:

- If a request is blocked by the web-based URL filter or FortiGuard filter, there is no further antiphishing scanning. Antiphishing scanning only happens after the web-based URL filter and FortiGuard filters allow the traffic.
  - If a submission matches an entry in the URL filter table that has an antiphishing action, the defined action is taken. No further FortiGuard category-based rules are applied.
  - Like firewall rules, the URL filter table and FortiGuard category-based antiphishing rules use a top-down priority. The rule that matches first is the one that is used.
-



In this example, URLs that match FortiGuard category 37 (social networking) will be blocked and other categories will be logged.

### To configure credential phishing prevention:

#### 1. Configure the corporate domain controller:

```
config credential-store domain-controller
  edit "win2016"
    set domain-name "corpserver.local"
    set username "Administrator"
    set password ENC password
    set ip <server_ip>
  next
end
```



The domain controller entry name must be the hostname of the DC (win2016 in the example). Both it and the domain name are case sensitive.

---

#### 2. Configure the antiphishing profile, which includes the FortiGuard category rule:

```
config webfilter profile
  edit "<profile-name>"
    set feature-set proxy
    ...
    config web
      ...
    end
    config antiphish
      set status enable
      set domain-controller "win2016"
      set default-action block
      set check-uri enable
      set check-basic-auth enable
      set max-body-len 65536
      config inspection-entries
        edit "inspect-37"
          set fortiguard-category 37
          set action block
        next
        edit "inspect-others"
          set fortiguard-category all
          set action log
        next
      end
      config custom-patterns
        edit "customer-name"
          set category username
        next
        edit "customer-passwd"
          set category password
        next
      end
    end
end
```

```

        ...
        set web-antiphishing-log enable
    next
end

```

- `check-uri` enables support for scanning HTTP GET URI parameters.
- `check-basic-auth` enables support for scanning the HTTP Basic Auth field.

### 3. Configure the URL filter to scan specific URLs.

The antiphish action is added to the URL filter table entry, and the URL filter is applied to the webfilter profile.

```

config webfilter urlfilter
    edit 1
        set name "antiphish-table"
        config entries
            edit 1
                set url "www.example.com"
                set type simple
                set antiphish-action block
                set status enable
                set referrer-host ''
            next
        end
    next
end
config webfilter profile
    edit "<profile-name>"
        config web
            set urlfilter-table 1
        end
        ...
    next
end

```

### 4. Optionally, define custom patterns to scan fields other than the built-in username and password keywords are needed:

```

config webfilter profile
    edit "<profile-name>"
        config custom-patterns
            edit "customer-name"
                set category username
            next
            edit "customer-passwd"
                set category password
            next
        end
    end
next
end

```

## Explicitly enable custom categories for web filter profiles, SSL/SSH inspection profiles, and proxy addresses - 6.4.2

In all web filter profiles, local and remote categories must be manually enabled.

When a new threat feed connector or web rating overrides in a custom category are created, they will not impact any web filters until the category's action is changed to *Monitor*, *Block*, *Warning*, or *Authenticate* in the specific web filter's settings. If a URL is in multiple enabled categories, the order of precedence is local categories, then remote categories, and then FortiGuard categories.

In SSL/SSH inspection profiles, local and remote categories must be explicitly selected to be exempt from SSL inspection. In proxy addresses, local and remote categories must be explicitly selected as URL categories for them to apply. In both settings, if a URL is in multiple selected categories, the order of precedence is local categories, then remote categories, and then FortiGuard categories.

## Web filter profiles

In this example, [www.fortinet.com](http://www.fortinet.com) is added to both a custom, or local, category (*Seriously*) and an external threat feed, or remote, category (*OnAworkComputer*). The local category action is set to *Monitor*, while the remote category action is set to *Block*. When a user browses to [www.fortinet.com](http://www.fortinet.com), the local category action takes precedence over both the remote category and the FortiGuard category (*Information Technology*), so the *Monitor* action is taken.

### To use local and remote categories in a web filter profile in the GUI:

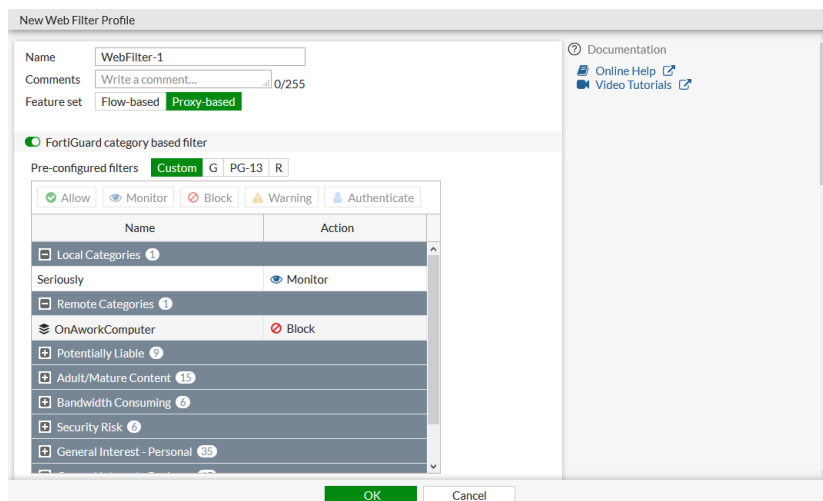
1. Go to **Security Profiles > Web Rating Overrides** and create a custom category and add URLs to it. See [Web rating override](#) for details.

2. Go to **Security Fabric > External Connectors** and create a *FortiGuard Category Threat Feed* external connector to import an external blacklist.

3. Go to **Security Profiles > Web Filter** and create or edit a web filter profile.
4. Set **Feature set** to *Proxy-based*.
5. Enable **FortiGuard category based filter** and change the action for the *Local Categories* and *Remote Categories* entries as needed. See [FortiGuard filter](#) for details.



When the action for a local or remote category is *Allow*, the category is disabled. The next category's action, in the order of preference, will be applied.



6. Configure the remaining settings as required.
7. Click OK.

#### To use local and remote categories in a web filter profile in the CLI:

1. Create a custom category and add URLs to it. See [Web rating override](#) for details.

```
config vdom
  edit root
    config webfilter ftgd-local-cat
      edit "Seriously"
        set id 140
      next
    end
    config webfilter ftgd-local-rating
      edit "www.fortinet.com"
        set rating 140
      next
    end
  next
end
```

2. Create a *FortiGuard Category Threat Feed* external connector to import an external blocklist:

```
config global
  config system external-resource
    edit "OnAworkComputer"
      set category 192
      set resource "https://192.168.0.5/lists/blocklist.txt"
    next
  end
end
```

3. Create or edit a web filter profile. See [FortiGuard filter](#) for details.  
Local categories have an ID range of 140 to 191. Remote categories have an ID range of 192 to 221.

```

config vdom
  edit root
    config webfilter profile
      edit "WebFilter-1"
        set feature-set proxy
        config ftgd-wf
          unset options
          config filters
            edit 12
              set category 12
              set action warning
            next
            ...
            edit 23
              set action warning
            next
            edit 140
              set category 140
            next
            edit 192
              set category 192
              set action block
            next
          end
        end
      next
    end
  next
end

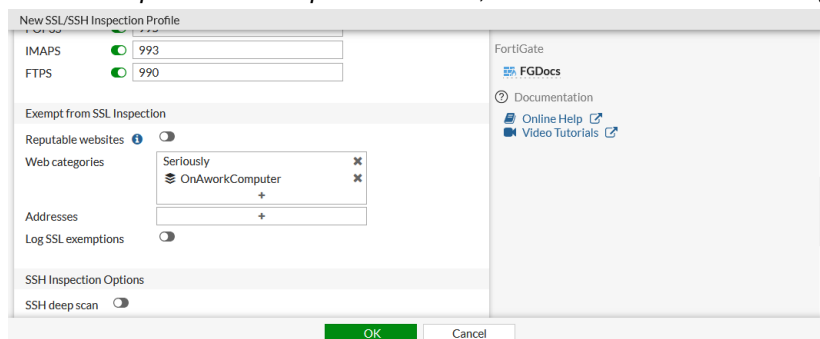
```

When a filter is added for the local and remote categories (140 and 192 in this example), the default action is monitor.

## SSL/SSH inspection profiles

To use local and remote categories in an SSL/SSH inspection profile to exempt the categories from SSL inspection in the GUI:

1. Go to *Security Profiles > SSL/SSH Inspection*.
2. Create a new profile or edit an existing one.
3. Ensure that *Inspection method* is *Full SSL Inspection*.
4. In the *Exempt from SSL Inspection* section, add the local and remote categories to the *Web categories* list .



5. Configure the remaining settings as required, then click *OK*.

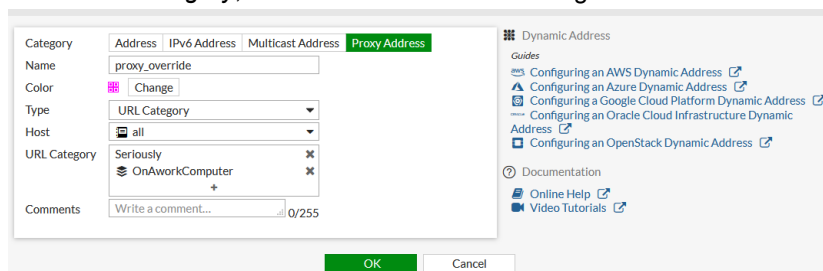
### To use local and remote categories in an SSL/SSH inspection profile to exempt the categories from SSL inspection in the CLI:

```
config firewall ssl-ssh-profile
  edit "SSL_Inspection"
    config https
      set ports 443
      set status deep-inspection
    end
    ...
    config ssl-exempt
      edit 1
        set fortiguard-category 140
      next
      edit 2
        set fortiguard-category 194
      next
    end
  next
end
```

## Proxy addresses

### To use local and remote categories in a proxy address in the GUI:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*, or edit an existing proxy address.
2. Set *Category* to *Proxy Address*.
3. Set *Type* to *URL Category*.
4. In the *URL Category*, add the local and remote categories.



5. Configure the remaining settings as required, then click **OK**.

### To use local and remote categories in a proxy address in the CLI:

```
config firewall proxy-address
  edit "proxy_override"
    set type category
    set host "all"
    set category 140 194
    set color 23
  next
end
```

## Configure web filter profiles in NGFW policy mode - 6.4.2

Web filters can be configured in NGFW policy mode, and used in security policies.

### To create in web filter profile when the FortiGate is in policy mode in the GUI:

1. Go to *Security Profiles > Web Filter* and click *Create New*.  
Only *Static URL Filter* options can be configured.
2. Enter a name for the profile and configure the remaining settings as required:

The screenshot shows the 'New Web Filter Profile' configuration window. The 'Name' field is set to 'webfilter-demo'. The 'Static URL Filter' section is expanded, showing 'Block invalid URLs' and 'URL Filter' both enabled. Below the 'URL Filter' section, there is a table with one entry:

URL	Type	Action	Status
*.bot*.com	Wildcard	Block	Enable

Below the table, 'Block malicious URLs discovered by FortiSandbox' is enabled. The 'Content Filter' section is also expanded, showing a table with four entries:

Pattern Type	Pattern	Language	Action	Status
Wildcard	gambling	Western	Block	Enable
Wildcard	news	Western	Block	Enable
Wildcard	test	Western	Block	Enable
Wildcard	example	Western	Block	Enable

The 'OK' button is highlighted in green at the bottom right of the window.

3. Click *OK*.

### To use the web filter profile in a security policy in the GUI:

1. Go to *Policy & Objects > Security Policy* and click *Create New*.
2. Enter a name for the policy, and configure the remaining settings as required.
3. Under *Security Profiles*, enable *Web Filter* and select the web filter.

The screenshot shows the 'New Policy' configuration window. The 'Name' field is set to 'policy-demo-1'. The 'Incoming Interface' is 'port2' and the 'Outgoing Interface' is 'port1'. The 'Source' and 'Destination' are both set to 'all'. The 'Schedule' is set to 'always'. The 'Service' is 'App Default'. The 'Application' list includes 'Network.Service' and 'Web.Client'. The 'URL Category' is set to 'all'. The 'Action' is set to 'ACCEPT'. The 'Firewall / Network Options' section shows 'Protocol Options' set to 'default'. The 'Security Profiles' section is expanded, showing 'AntiVirus' disabled, 'Web Filter' enabled and set to 'webfilter-demo', 'IPS' disabled, and 'File Filter' disabled. The 'OK' button is highlighted in green at the bottom right of the window.

4. Click *OK*.

**To create in web filter profile when the FortiGate is in policy mode in the CLI:****1. Configure a URL filter:**

```
config webfilter urlfilter
  edit 1
    set name "Auto-webfilter-urlfilter_bwv7ilr83"
    config entries
      edit 1
        set url "*.bot*.com"
        set type wildcard
        set action block
      next
    end
  next
end
```

**2. Configure content filters:**

```
config webfilter content
  edit 1
    set name "Auto-webfilter-content_mqqyssuxd"
    config entries
      edit "gambling"
        set status enable
      next
      edit "news"
        set status enable
      next
      edit "test"
        set status enable
      next
      edit "example"
        set status enable
      next
    end
  next
end
```

**3. Configure the web filter profile:**

```
config webfilter profile
  edit "webfilter-demo"
    set options block-invalid-url
    config web
      set bword-table 1
      set urlfilter-table 1
      set blacklist enable
    end
  next
end
```

**To use the web filter profile in a security policy in the CLI:**

```
config firewall security-policy
  edit 1
    set name "policy-demo-1"
    set srcintf "port2"
```



```

        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set webfilter-profile "webfilter-demo"
        set app-category 15 25
    next
end

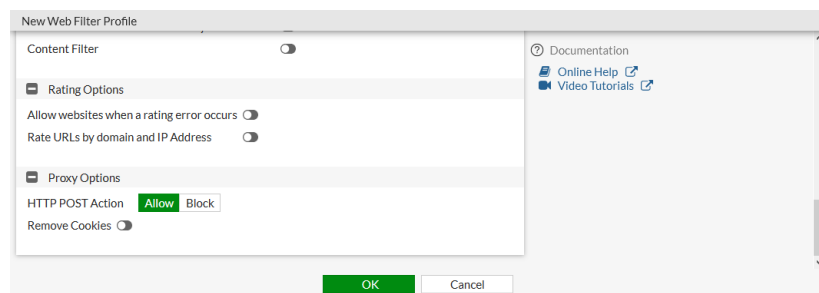
```

## Remove the option to rate images by URL in Web filter profiles - 6.4.3

The option to rate images by their URL in web filter profiles is removed.

Search engines fetch searched images from their own caches, preventing FortiOS from detecting the original URL of the image, and making the rated category incorrect.

The options is removed from the *Ratings Options* section when configuring a web filter profile in the GUI:



The `rate-image-urls` command is removed from the CLI:

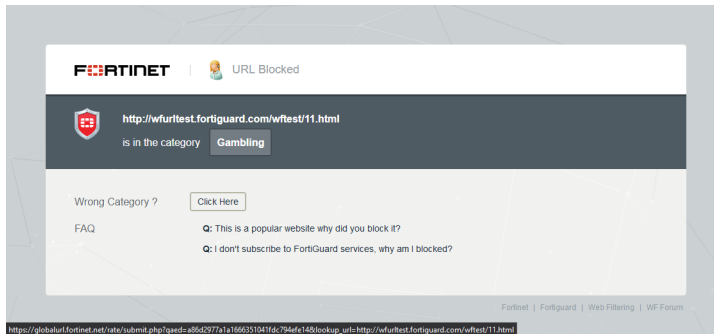
```

config webfilter profile
    edit "profile"
        config ftgd-wf
            set options {options}
            set exempt-quota <string>
            set ovrd <string>
            set max-quota-timeout <integer>
            set rate-javascript-urls {enable | disable}
            set rate-css-urls {enable | disable}
            set rate-crl-urls {enable | disable}
        end
    next
end

```

## Rating submission link on web filter block and warning pages - 6.4.5

The URL re-evaluation link on web filter block and warning pages points to <https://globalurl.fortinet.net>.



Clicking *Click Here* opens the re-evaluation request page:

## IPS

This section includes information about IPS related new features:

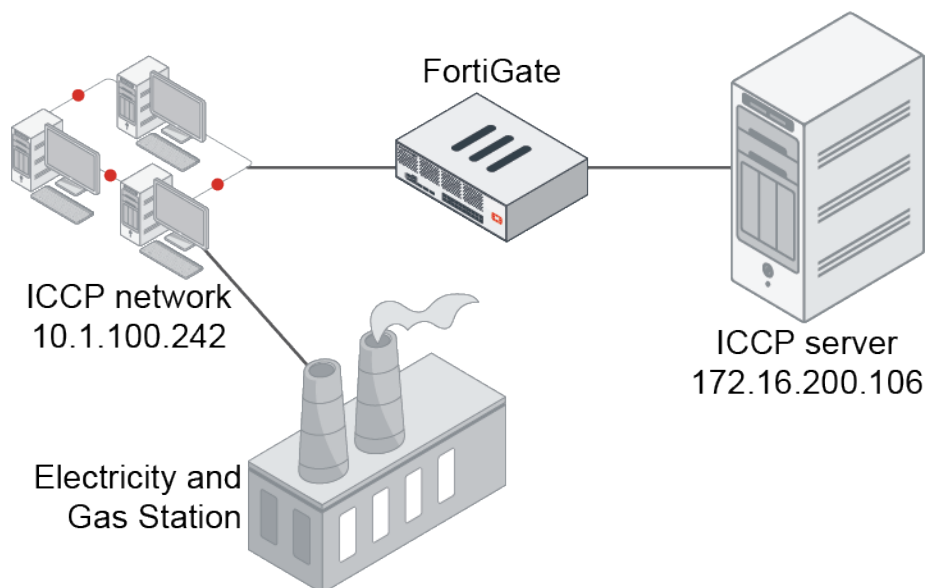
- [Detecting IEC 61850 MMS protocol in IPS on page 316](#)
- [IPS signature filter options 6.4.2 on page 318](#)

## Detecting IEC 61850 MMS protocol in IPS

IEC 61850 is a SCADA protocol whose services are mapped to a number of protocols, including MMS services. MMS/ICCP detection is supported in IPS. The purpose of the MMS dissectors is to identify every IEC 61850 service to distinguish different MMS/ICCP messages. IPS engine 6.0.12 and later support MMS dissectors.

The following scenarios are also supported:

- Multiple MMS PDUs are transferred in one TCP payload, and the IPS engine identifies individuals.
- An MMS message is split over multiple TCP segments, where MMS runs over COTP segments.
- ICCP/TASE.2 that also uses MMS transport (ISO transport over TCP for ICCP) is detected.



Industrial signatures must be enabled in the global IPS settings to receive MMS/ICCP signatures. By default, industrial signatures are excluded.

```
config ips global
    set exclude-signatures none
end
```

Below are some industrial signatures for MMS/ICCP messages that can be detected by the IPS engine. This is not an exhaustive list.

- MMS\_GetNameList.Request
- MMS\_GetNamedVariableListAttributes.Request
- MMS\_GetVariableAccessAttributes.Request
- MMS\_Identify.Request
- MMS\_Initiate.Request
- MMS\_Read.Request
- MMS\_Reset.Request
- ICCP\_Transfer.Reporting
- ICCP\_Create.Dataset
- ICCP\_Abort
- ICCP\_Start.Transfer.DSTransferSet
- ICCP\_Get.Dataset.Element.Values
- ICCP\_Get.Next.DSTransfer.Set.Value
- ICCP\_Delete.Dataset
- ICCP\_Start.Transfer.IMTransferSet

### Diagnose command

The COTP dissector adds support for identifying every MMS PDU, and let the IPS engine separate them, like the Modbus and IEC-104 services for example.

```
# diagnose ips debug enable all
# diagnose debug enable
```

```
[284@78]ips_17_dsct_processor: serial=8142 create: cotp
[284@78]ips_17_dsct_processor: serial=8142 create: iec104
[284@78]ips_17_dsct_processor: serial=8142 create: modbus
```

## Log samples

MMS dissectors can be triggered, and MMS/ICCP signatures can be monitored and logged.

### Log samples:

```
date=2020-03-26 time=15:51:10 logid="1059028704" type="utm" subtype="app-ctrl"
eventtype="signature" level="information" vd="vd1" eventtime=1585263070836106492 tz="-0700"
appid=43699 srcip=10.1.100.242 dstip=172.16.200.106 srcport=50963 dstport=102
srcintf="port13" srcintfrole="undefined" dstintf="port14" dstintfrole="undefined" proto=6
service="tcp/26112" direction="outgoing" policyid=1 sessionid=2711 applist="test"
action="pass" appcat="Industrial" app="MMS_Read.Request" incidentserialno=376610508
msg="Industrial: MMS_Read.Request," apprisk="elevated"
```

```
date=2020-03-26 time=16:15:45 logid="1059028704" type="utm" subtype="app-ctrl"
eventtype="signature" level="information" vd="vd1" eventtime=1585091746264983273 tz="-0700"
appid=44684 srcip=10.1.100.242 dstip=172.16.200.106 srcport=41665 dstport=102
srcintf="port13" srcintfrole="undefined" dstintf="port14" dstintfrole="undefined" proto=6
service="tcp/26112" direction="incoming" policyid=1 sessionid=194463 applist="test"
action="pass" appcat="Industrial" app="ICCP_Transfer.Reporting" incidentserialno=762763993
msg="Industrial: ICCP_Transfer.Reporting," apprisk="elevated"
```

## IPS signature filter options - 6.4.2

IPS signature filter options include hold-time and CVE pattern.

### hold-time

The hold-time option allows you to set the amount of time that signatures are held after a FortiGuard IPS signature update per VDOM. During the holding period, the signature's mode is *monitor*. The new signatures are enabled after the hold-time, to avoid false positives.

The hold-time can be from 0 days and 0 hours (default) up to 7 days, in the format ##d##h.

### To configure the amount of time to hold and monitor IPS signatures:

```
config system ips
    set signature-hold-time 3d12h
    set override-signature-hold-by-id enable
end
```

When a signature that is on hold is matched, the log will include the message `signature is on hold`:

```
date=2010-07-06 time=00:00:57 logid="0419016384" type="utm" subtype="ips"
eventtype="signature" level="alert" vd="vd1" eventtime=1278399657778481842 tz="-0700"
severity="info" srcip=10.1.100.22 srccountry="Reserved" dstip=172.16.200.55 srcintf="port13"
srcintfrole="undefined" dstintf="port14" dstintfrole="undefined" sessionid=3620
action="detected" proto=6 service="HTTP" policyid=1 attack="Eicar.Virus.Test.File"
srcport=52170 dstport=80 hostname="172.16.200.55" url="/virus/eicar" direction="incoming"
```

```
attackid=29844 profile="test" ref="http://www.fortinet.com/ids/VID29844"
incidentserialno=25165825 msg="file_transfer: Eicar.Virus.Test.File, (signature is on hold)"
```

### To view signatures being held by rule ID 29844 on the vd1 VDOM:

```
# diagnose ips signature on-hold vd1 29844
Rule: 29844, attack_id: 58886, last updated: 20170411
Rule: 29844, attack_id: 59517, last updated: 20170411
Rule: 29844, attack_id: 60105, last updated: 20170411
```

### To view all help signatures on the vd1 VDOM:

```
# diagnose ips signature on-hold vd1
Rule: 17541, attack_id: 20899, last updated: 20140423
Rule: 17557, attack_id: 20934, last updated: 20140423
Rule: 17559, attack_id: 20932, last updated: 20140423
Rule: 17560, attack_id: 20933, last updated: 20140423
Rule: 17562, attack_id: 20928, last updated: 20170908
Rule: 17677, attack_id: 21187, last updated: 20171106
Rule: 17713, attack_id: 43756, last updated: 20140424
Rule: 17759, attack_id: 21298, last updated: 20140423
...
```

## CVE pattern

The CVE pattern option allows you to filter IPS signatures based on CVE IDs or with a CVE wildcard, ensuring that any signatures tagged with that CVE are automatically included.

### To configure CVE patterns for CVE-2010-0177 and all CVE-2017 CVEs:

```
config ips sensor
  edit "cve"
    set comment "cve"
    config entries
      edit 1
        set cve "cve-2010-0177"
        set status enable
        set log-packet enable
        set action block
      next
      edit 2
        set cve "cve-2017"
        set action reset
      next
    end
  next
end
```

For example, the CVE of the IPS signature *Mozilla.Firefox.PluginArray.NsMimeType.Code.Execution* is CVE-2010-0177. This matches the CVE filter in the IPS sensor, so traffic is blocked and logged:

```
date=2020-07-13 time=15:44:56 logid="0419016384" type="utm" subtype="ips"
eventtype="signature" level="alert" vd="vd1" eventtime=159459389666145871 tz="-0700"
severity="critical" srcip=10.1.100.22 srccountry="Reserved" dstip=172.16.200.55
srcintf="port2" srcintfrole="undefined" dstintf="port1" dstintfrole="undefined"
```

```

sessionid=1638 action="dropped" proto=6 service="HTTPS" policyid=1
attack="Mozilla.Firefox.PluginArray.NsMimeType.Code.Execution" srcport=58298 dstport=443
hostname="172.16.200.55" url="/Mozilla" direction="incoming" attackid=20853 profile="sensor-
1" ref="http://www.fortinet.com/ids/VID20853" incidentserialno=124780667 msg="web_client:
Mozilla.Firefox.PluginArray.NsMimeType.Code.Execution," crscore=50 craction=4096
crlevel="critical"

```

## Others

This section includes information about other security profile related new features:

- [Redirect to WAD after handshake completion on page 320](#)
- [ICAP response filtering on page 321](#)
- [Separate file filter into a standalone profile 6.4.1 on page 323](#)
- [Handling SSL offloaded traffic from an external decryption device in flow mode 6.4.4 on page 325](#)

## Redirect to WAD after handshake completion

In a proxy-based policy, the TCP connection is proxied by the FortiGate. A TCP 3-way handshake can be established with the client even though the server did not complete the handshake.

This option uses IPS to handle the initial TCP 3-way handshake. It rebuilds the sockets and redirects the session back to proxy only when the handshake with the server is established.

### To enable proxy after a TCP handshake in an SSL/SSH profile:

```

config firewall ssl-ssh-profile
  edit "test"
    config https
      set ports 443
      set status certificate-inspection
      set proxy-after-tcp-handshake enable
    end
    .....
  next
end

```

### To enable proxy after a TCP handshake in protocol options:

```

config firewall profile-protocol-options
  edit "test"
    config http
      set ports 80
      set proxy-after-tcp-handshake enable
      unset options
      unset post-lang
    end
    ....
  next
end

```

## ICAP response filtering

ICAP HTTP responses can be forwarded or bypassed based on the HTTP header value and status code.

When configuring the ICAP profile, if `response` is enabled, the `respmod-default-action` option can be configured:

- If `respmod-default-action` is set to `forward`, FortiGate will treat every HTTP response, and send ICAP requests to the ICAP server.
- If `respmod-default-action` is set to `bypass`, FortiGate will only send ICAP requests if the HTTP response matches the defined rules, and the rule's action is set to `forward`.

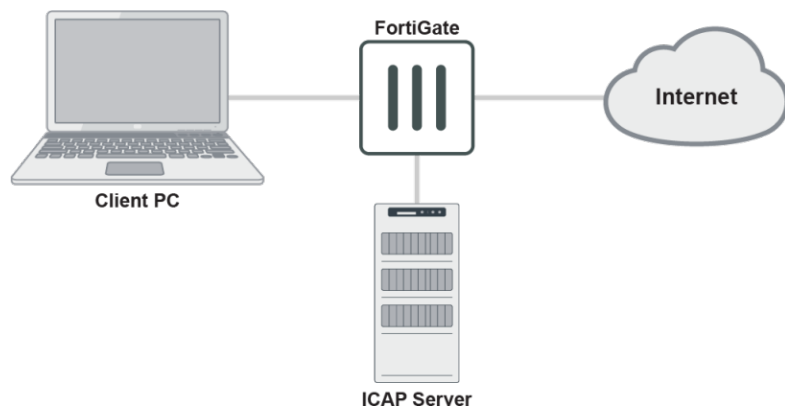
When configuring a response rule:

- The `http-resp-status-code` option is configured to specific HTTP response codes. If the HTTP response has any one of the configured values, then the rule takes effect.
- Multiple header value matching groups can be configured. If the header value matches one of the groups, then the rule takes effect.
- If both status codes and header values are specified in a rule, the response must match at least one of each.

The UTM ICAP log category is used for logging actions when FortiGate encounters errors with the ICAP server, such as no service, unreachable, error response code, or timeout. If an error occurs, a traffic log and an associated UTM ICAP log will be created.

### Example

The FortiGate acts as a gateway for the client PC, and connects to a reachable ICAP server. The ICAP server can be in NAT, transparent, or proxy mode.



In this example, client request HTTP responses will be forwarded to the ICAP server from all hosts if they have an HTTP status code of 200, 301, or 302, and have `content-type: image/jpeg` in their header.

#### To configure an ICAP profile with HTTP response rules:

```

config icap profile
  edit "icap_profile2"
    set request disable
    set response enable
    set streaming-content-bypass disable
    set preview disable
    set response-server "icap_server1"
  
```

```

set response-failure error
set response-path ''
set methods delete get head options post put trace other
set response-req-hdr disable
set respmod-default-action bypass
config respmod-forward-rules
    edit "rule2"
        set host "all"
        set action forward
        set http-resp-status-code 200 301 302
        config header-group
            edit 2
                set header-name "content-type"
                set header "image/jpeg"
            next
        end
    next
end
next
end

```

### To view the logs if an error occurs:

#### 1. View the traffic log:

```

# execute log filter category 0
# execute log display
1 logs found.
1 logs returned.

1: date=2019-10-25 time=17:43:47 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1572050627037314464 tz="-0700" srcip=10.1.100.145
srcport=47968 srcintf="port1" srcintfrole="undefined" dstip=172.16.200.46 dstport=80
dstintf="port2" dstintfrole="undefined" poluid="a4d5324e-f6c3-51e9-ce2d-f360994fb547"
sessionid=43549 proto=6 action="close" policyid=1 policytype="policy" service="HTTP"
dstcountry="Reserved" srccountry="Reserved" trandisp="snat" transip=172.16.200.1
transport=47968 duration=1 sentbyte=485 rcvbyte=398 sentpkt=6 rcvpkt=5
appcat="unscanned" wanin=478 wanout=165 lanin=165 lanout=165 utmaction="block"
counticap=1 crscore=5 craction=262144 crlevel="low" utmref=65532-0

```

#### 2. View the UTM ICAP log:

```

# execute log filter category 20
# execute log display
1 logs found.
1 logs returned.

1: date=2019-10-25 time=17:43:46 logid="2000060000" type="utm" subtype="icap"
eventtype="icap" level="warning" vd="vdom1" eventtime=1572050626010097145 tz="-0700"
msg="Request blocked due to ICAP server error" service="HTTP" srcip=10.1.100.145
dstip=172.16.200.46 srcport=47968 dstport=80 srcintf="port1" srcintfrole="undefined"
dstintf="port2" dstintfrole="undefined" policyid=1 sessionid=43549 proto=6
action="blocked" profile="icap_profile1" url="/icap_test/"

```

The logs show that, in this case, the ICAP services stopped before the access. When the client tried to access HTTP and ICAP took effect, the FortiGate sent the ICAP request to the ICAP server and received an error. The client sees a 502



*Bad Gateway* message, and FortiGate writes the two logs. In the GUI, the logged traffic is displayed as *Result: Deny: UTM Blocked*.

## Separate file filter into a standalone profile - 6.4.1

The previously embedded file filter within web filter, email filter, SSH inspection, and CIFS has moved to a standalone profile. The file filter can be applied directly to firewall policies and supports various traffic protocols in proxy or flow mode.

When upgrading to FortiOS 6.4.1, existing embedded file filter rules (web filter, email filter, SSH inspection, and CIFS) that are not used in any policies or profile groups will have new file filter profiles created for them. Any firewall policies, proxy policies, or profile groups with existing embedded file filter rules will have new file filter profiles created for them.

### To configure a file filter in the GUI:

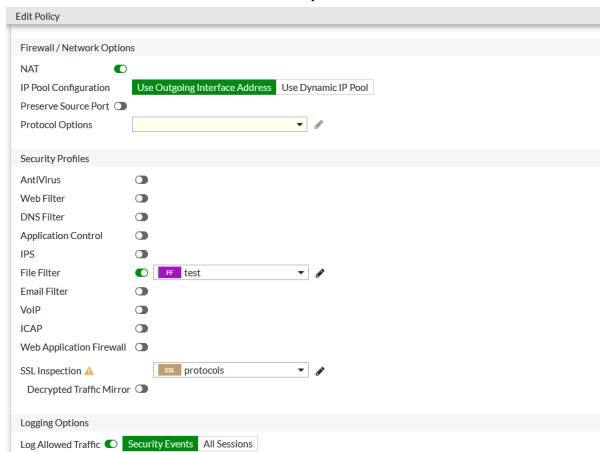
1. Configure the filter profile:
  - a. Go to *Security Profiles > File Filter* and click *Create New*.
  - b. Select a *Feature set*.
  - c. In the *Rules* section, click *Create New*.
  - d. Configure the settings as needed.
  - e. Click *OK* to save the rule.

- f. Optionally, create more rules if needed.
  - g. Click *OK* to save the filter profile.

Rule	Comments	Traffic	Protocols	Match Files	Action	File Types
r2		Outgoing	HTTP FTP	Any	Block	sfs tar
r1		Both	HTTP FTP	Any	Monitor	.net 7z
r3		Both	HTTP FTP	Any	Block	binhex

2. Apply the filter to a policy:
  - a. Go to *Policy & Objects > Firewall Policy*, and edit an existing policy or create a new one.
  - b. In the *Security Profiles* section, enable *File Filter*.

- c. Select the filter from the dropdown box.



- d. Configure the other settings as needed.  
e. Click OK.

### To configure a file filter in the CLI:

1. Configure the file filter profile:

```
config file-filter profile
  edit "test"
    set comment ''
    set feature-set flow
    set replacemsg-group ''
    set log enable
    set scan-archive-contents enable
    config rules
      edit "r2"
        set comment ''
        set protocol http ftp smtp imap pop3 cifs
        set action block
        set direction outgoing
        set password-protected any
        set file-type "sis" "tar" "tiff" "torrent" "upx" "uue" "wav" "wma" "xar"
        "xz" "zip"
      next
      edit "r1"
        set comment ''
        set protocol http ftp smtp imap pop3 cifs
        set action log-only
        set direction any
        set password-protected any
        set file-type ".net" "7z" "activemime" "arj" "aspack" "avi" "base64"
        "bat" "binhex" "bmp" "bzip" "bzip2"
      next
      edit "r3"
        set comment ''
        set protocol http ftp smtp imap pop3
        set action block
        set direction any
        set password-protected any
```

```

        set file-type "binhex"
    next
end
next
end

```

## 2. Apply the filter to a policy:

```

config firewall policy
    edit 1
        set name "filefilter-policy"
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set profile-protocol-options "protocol"
        set ssl-ssh-profile "protocols"
        set file-filter-profile "test"
        set auto-asic-offload disable
        set np-acceleration disable
        set nat enable
    next
end

```

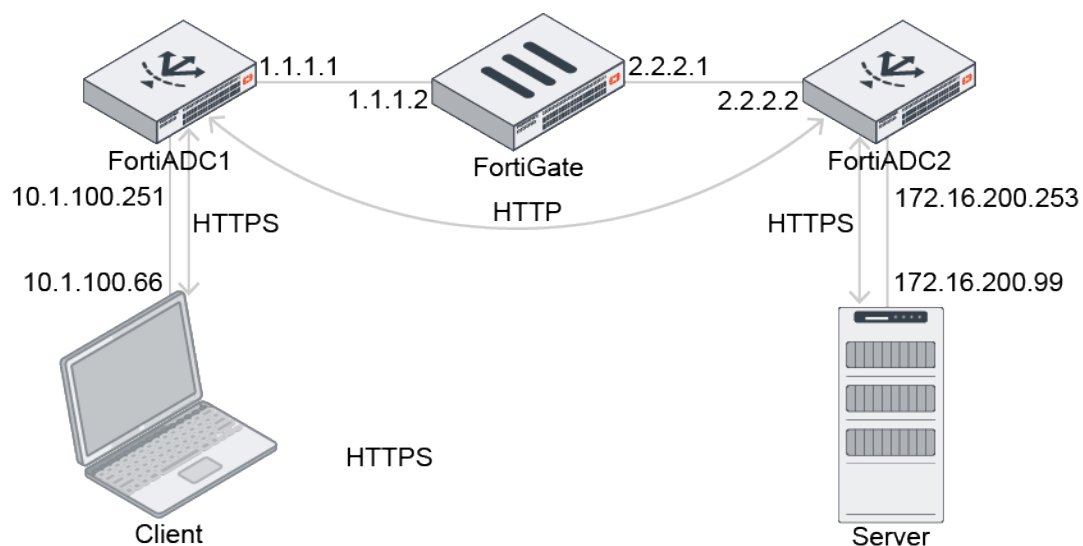
## Handling SSL offloaded traffic from an external decryption device in flow mode - 6.4.4

In scenarios where the FortiGate is sandwiched between load-balancers and SSL processing is offloaded on the external load-balancers, the FortiGate can perform scanning on the unencrypted traffic by specifying the `ssl-offloaded` option in firewall `profile-protocol-options`. Previously, this was only supported in proxy mode. Now it is supported in proxy and flow mode.

### Sample topology

In this example, the FortiGate is between two FortiADCs and in SSL offload sandwich mode. The FortiGate receives plain text from ADC1 and forwards plain text to ADC2. There is no encrypted traffic passing through the FortiGate.

The client sends HTTPS traffic to ADC1, which then decrypts the traffic and sends HTTP to the FortiGate. The FortiGate forwards HTTP to ADC2, and the ADC2 re-encrypts the traffic to HTTPS.



### To configure SSL offloading:

```

config firewall profile-protocol-options
  edit "default-clone"
    config http
      set ports 80
      unset options
      unset post-lang
      set ssl-offloaded yes
    end
    config ftp
      set ports 21
      set options splice
      set ssl-offloaded yes
    end
    config imap
      set ports 143
      set options fragmail
      set ssl-offloaded yes
    end
    config pop3
      set ports 110
      set options fragmail
      set ssl-offloaded yes
    end
    config smtp
      set ports 25
      set options fragmail splice
      set ssl-offloaded yes
    end
  next
end

```

### Verifying the packet captures

The ADC1 incoming port capture shows that ADC1 receives HTTPS traffic:

No.	Time	Source	Destination	Protocol	Length	Info
20	8.538335	10.1.100.66	172.16.200.99	TCP	74	49818 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2672317962 TSecr=0 WS=128
21	8.538488	172.16.200.99	10.1.100.66	TCP	74	443 → 49818 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=880725085 TSecr=2672317962 WS=512
22	8.538530	10.1.100.66	172.16.200.99	TCP	66	49818 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2672317962 TSecr=880725085
23	8.540564	10.1.100.66	172.16.200.99	TLSv1.2	583	Client Hello
24	8.546120	172.16.200.99	10.1.100.66	TLSv1.2	1740	Server Hello, Certificate, Server Key Exchange, Server Hello Done
25	8.546279	10.1.100.66	172.16.200.99	TCP	66	49818 → 443 [ACK] Seq=518 Ack=1675 Win=63488 Len=0 TSval=2672317970 TSecr=880725093
26	8.547757	10.1.100.66	172.16.200.99	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27	8.547968	172.16.200.99	10.1.100.66	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
28	8.549545	10.1.100.66	172.16.200.99	TLSv1.2	172	Application Data
29	8.557688	172.16.200.99	10.1.100.66	TLSv1.2	418	Application Data
30	8.559656	10.1.100.66	172.16.200.99	TLSv1.2	97	Encrypted Alert
31	8.559730	172.16.200.99	10.1.100.66	TLSv1.2	97	Encrypted Alert

The ADC1 outgoing port capture shows that ADC1 decrypts traffic and forwards HTTP traffic to the FortiGate:

No.	Time	Source	Destination	Protocol	Length	Info
9	9.499689	10.1.100.66	172.16.200.99	TCP	74	61516 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=361768736 TSecr=0 WS=512
10	9.500005	172.16.200.99	10.1.100.66	TCP	74	80 → 61516 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2517238757 TSecr=361768736 WS=512
11	9.500048	10.1.100.66	172.16.200.99	HTTP	143	GET / HTTP/1.1
12	9.507596	172.16.200.99	10.1.100.66	HTTP	389	HTTP/1.1 200 OK (text/html)
> Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)						
> Ethernet II, Src: Vmware_94:15:60 (00:0c:29:94:15:60), Dst: Vmware_9f:87:a3 (00:0c:29:9f:87:a3)						
> Internet Protocol Version 4, Src: 10.1.100.66, Dst: 172.16.200.99						
> Transmission Control Protocol, Src Port: 61516, Dst Port: 80, Seq: 0, Len: 0						

The FortiGate's incoming and outgoing port captures show that HTTP traffic passes through the FortiGate:

No.	Time	Source	Destination	Protocol	Length	Info
5	4.529844	10.1.100.66	172.16.200.99	TCP	74	61516 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=361768736 TSecr=0 WS=512
6	4.529904	172.16.200.99	10.1.100.66	TCP	74	80 → 61516 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2517238757 TSecr=361768736 WS=512
7	4.525194	10.1.100.66	172.16.200.99	HTTP	143	GET / HTTP/1.1
8	4.532691	172.16.200.99	10.1.100.66	HTTP	389	HTTP/1.1 200 OK (text/html)
> Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)						
> Ethernet II, Src: Vmware_94:15:60 (00:0c:29:94:15:60), Dst: Vmware_9f:87:a3 (00:0c:29:9f:87:a3)						
> Internet Protocol Version 4, Src: 10.1.100.66, Dst: 172.16.200.99						
> Transmission Control Protocol, Src Port: 61516, Dst Port: 80, Seq: 0, Len: 0						

No.	Time	Source	Destination	Protocol	Length	Info
13	3.688108	2.2.2.1	172.16.200.99	TCP	74	61516 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=361768736 TSecr=0 WS=512
14	3.688209	172.16.200.99	2.2.2.1	TCP	74	80 → 61516 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2517238757 TSecr=361768736 WS=512
15	3.688414	2.2.2.1	172.16.200.99	HTTP	143	GET / HTTP/1.1
16	3.695791	172.16.200.99	2.2.2.1	HTTP	389	HTTP/1.1 200 OK (text/html)
> Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)						
> Ethernet II, Src: Vmware_9f:87:ad (00:0c:29:9f:87:ad), Dst: Vmware_52:b2:91 (00:0c:29:52:b2:91)						
> Internet Protocol Version 4, Src: 2.2.2.1, Dst: 172.16.200.99						
> Transmission Control Protocol, Src Port: 61516, Dst Port: 80, Seq: 0, Len: 0						

The ADC2 incoming port capture shows that the ADC2 receives HTTP traffic:

No.	Time	Source	Destination	Protocol	Length	Info
38	11.585717	2.2.2.1	172.16.200.99	TCP	74	61516 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=361768736 TSecr=0 WS=512
39	11.585757	172.16.200.99	2.2.2.1	TCP	74	80 → 61516 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=361768736 WS=512
40	11.586012	2.2.2.1	172.16.200.99	HTTP	143	GET / HTTP/1.1
41	11.593343	172.16.200.99	2.2.2.1	HTTP	389	HTTP/1.1 200 OK (text/html)
> Frame 38: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)						
> Ethernet II, Src: Vmware_9f:87:ad (00:0c:29:9f:87:ad), Dst: Vmware_52:b2:91 (00:0c:29:52:b2:91)						
> Internet Protocol Version 4, Src: 2.2.2.1, Dst: 172.16.200.99						
> Transmission Control Protocol, Src Port: 61516, Dst Port: 80, Seq: 0, Len: 0						

The ADC2 outgoing port capture shows that ADC2 forwards HTTPS traffic to the server:

No.	Time	Source	Destination	Protocol	Length	Info
56	11.896674	2.2.2.1	172.16.200.99	TCP	74	57602 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1423415082 TSecr=0 WS=512
57	11.896813	172.16.200.99	2.2.2.1	TCP	74	443 → 57602 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1140593656 TSecr=1423415082 WS=128
58	11.896841	2.2.2.1	172.16.200.99	TLSv1.2	258	Client Hello
59	11.896966	172.16.200.99	2.2.2.1	TCP	66	443 → 57602 [ACK] Seq=1 Ack=193 Win=65024 Len=0 TSval=1140593656 TSecr=1423415082
60	11.902562	172.16.200.99	2.2.2.1	TLSv1.2	1514	Server Hello
61	11.902572	172.16.200.99	2.2.2.1	TLSv1.2	669	Certificate, Server Key Exchange, Server Hello Done
62	11.902580	2.2.2.1	172.16.200.99	TCP	66	57602 → 443 [ACK] Seq=193 Ack=2052 Win=35328 Len=0 TSval=1423415088 TSecr=1140593661
63	11.903194	2.2.2.1	172.16.200.99	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
64	11.903415	172.16.200.99	2.2.2.1	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
65	11.903491	2.2.2.1	172.16.200.99	TLSv1.2	172	Application Data
66	11.903752	172.16.200.99	2.2.2.1	TLSv1.2	418	Application Data
> Frame 58: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)						
> Ethernet II, Src: Vmware_52:b2:9b (00:0c:29:52:b2:9b), Dst: Vmware_e2:22:3b (00:0c:29:e2:22:3b)						
> Internet Protocol Version 4, Src: 2.2.2.1, Dst: 172.16.200.99						
> Transmission Control Protocol, Src Port: 57602, Dst Port: 443, Seq: 1, Ack: 1, Len: 192						
> Transport Layer Security						

# VPN

This section includes information about VPN related new features:

- [IPsec and SSL VPN on page 328](#)

## IPsec and SSL VPN

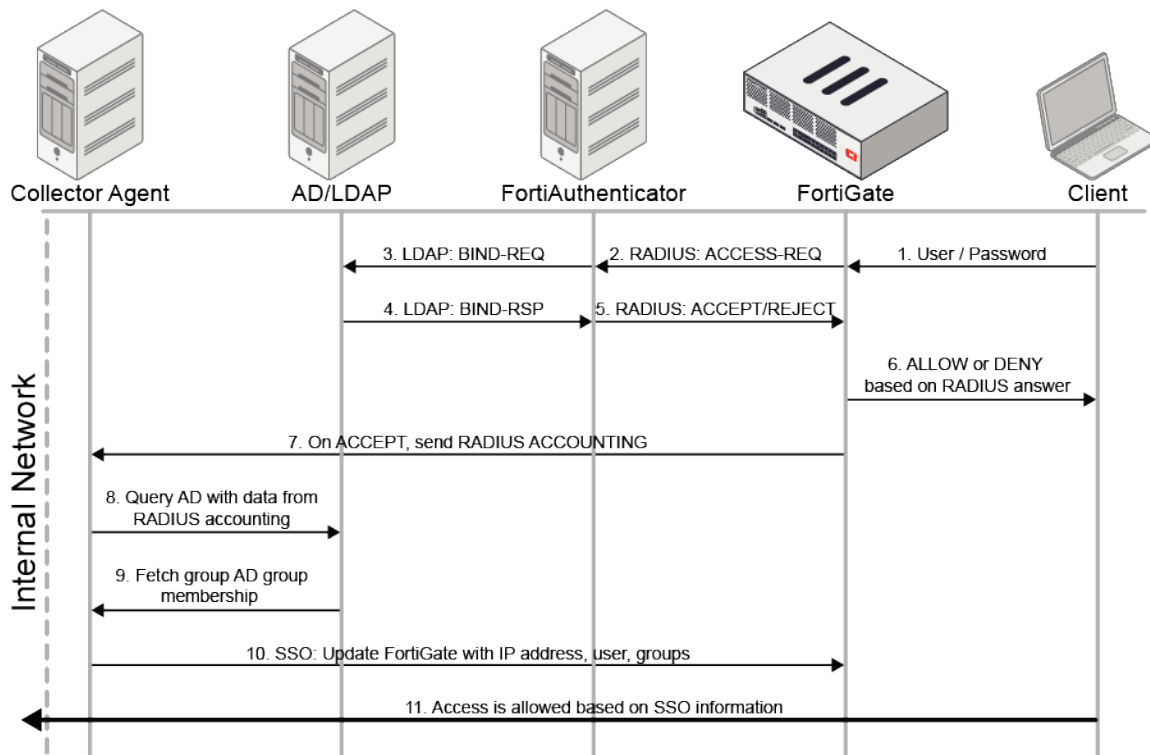
This section includes information about IPsec and SSL VPN related new features:

- [Dynamic address support for SSL VPN policies on page 328](#)
- [NAS-IP support per SSL VPN realm on page 337](#)
- [Support defining gateway IP addresses in IPsec with mode-config and DHCP on page 339](#)
- [Provision SSL VPN users in FortiClient Mobile with an email or SMS message 6.4.2 on page 341](#)
- [Configure DSCP for IPsec tunnels 6.4.3 on page 341](#)

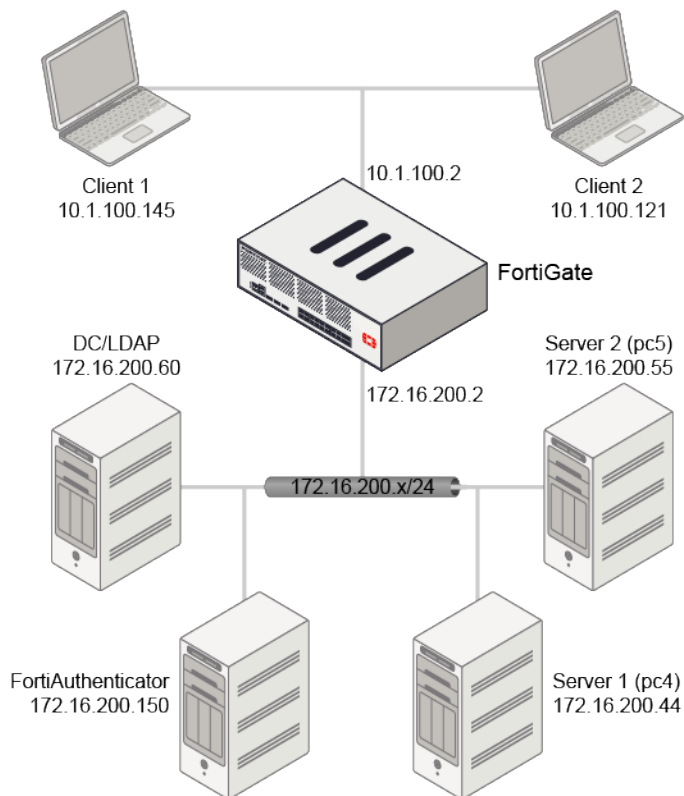
## Dynamic address support for SSL VPN policies

Dynamic SSO user groups can be used in place of address objects when configuring SSL VPN policies. This allows dynamic IP addresses to be used in SSL VPN policies. A remote user group can be used for authentication while an FSSO group is separately used for authorization. Using a dummy policy for remote user authentication and a policy for FSSO group authorization, FSSO can be used with SSL VPN tunnels

This image shows the authentication and authorization flow:



In this example, FortiAuthenticator is used as a RADIUS server. It uses a remote AD/LDAP server for authentication, then returns the authentication results to the FortiGate. This allows the client to have a dynamic IP address after successful authentication.

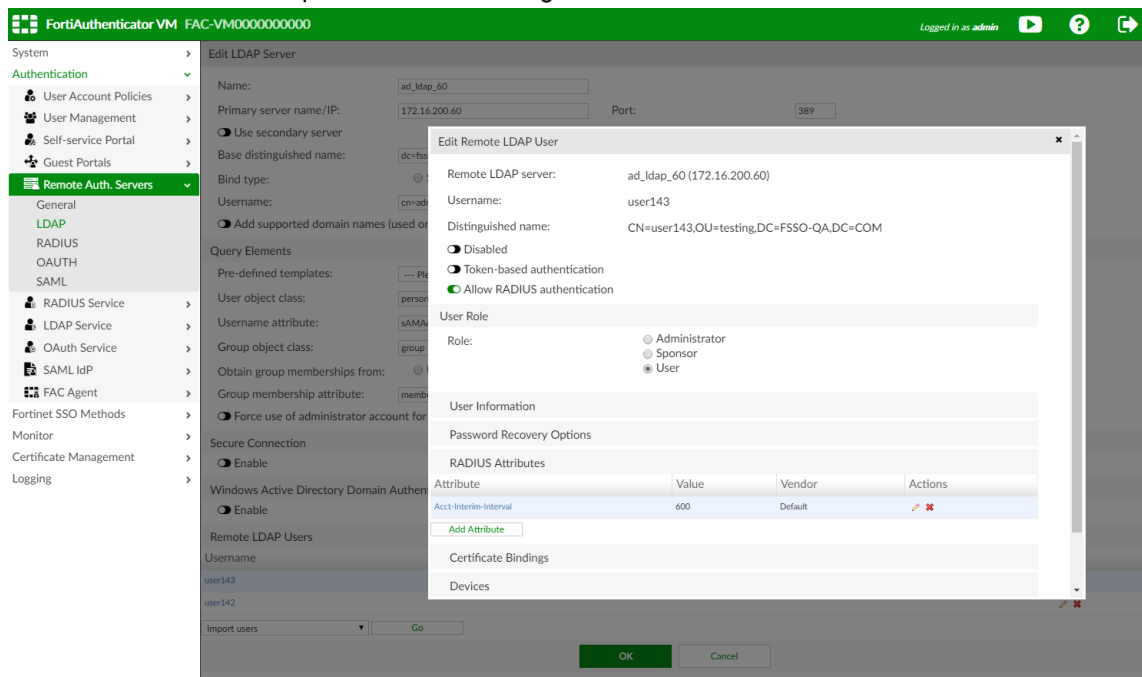


First, on the LDAP server, create two users each in their own group, *user142* in group *pc\_group1*, and *user143* in group *pc\_group2*.

## Configure the FortiAuthenticator

To add a remote LDAP server and users on the FortiAuthenticator:

1. Go to *Authentication > Remote Auth. Servers > LDAP*.
2. Click *Create New*.
3. Set the following:
  - *Name*: *ad\_ldap\_60*
  - *Primary server name/IP*: *172.16.200.60*
  - *Base distinguished name*: *dc=fsso-qa,dc=com*
  - *Bind type*: *Regular*
  - *Username*: *cn=administrator,cn=User*
  - *Password*: <enter a password>
4. Click *OK*.
5. Edit the new LDAP server.
6. Import the remote LDAP users.
7. Edit each user to confirm that they have the RADIUS attribute *Acct-Interim-Interval*. This attribute is used by FortiGate to send interim update account messages to the RADIUS server.



To create a RADIUS client for FortiGate as a remote authentication server:

1. Go to *Authentication > RADIUS Service > Clients*.
2. Click *Create New*.

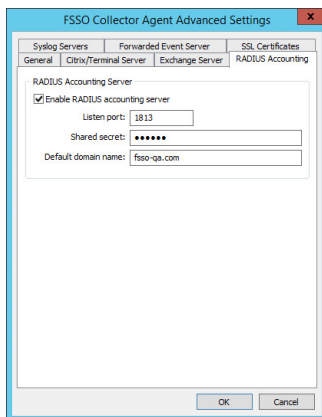


3. Set the following:
  - *Name*: *fsso\_ldap*
  - *Client address*: *Range 172.16.200.1~172.16.200.10*
  - *Secret*: <enter a password>
4. In the *Realms* table, set the realm to the LDAP server that was just added: *ad\_ldap\_60*.
5. Click **OK**.  
FortiAuthenticator can now be used as a RADIUS server, and the authentication credentials all come from the DC/LDAP server.

## Fortinet Single Sign-On Collector Agent

### To configure the Fortinet Single Sign-On Collector Agent:

1. Select *Require authenticated connection from FortiGate* and enter a *Password*.
2. Click *Advanced Settings*.
3. Select the *RADIUS Accounting* tab.
4. Select *Enable RADIUS accounting server* and set the *Shared secret*.



5. Click **OK**, then click *Save & close*.  
The collector agent can now accept accounting requests from FortiGate, and retrieve the IP addresses and usernames of SSL VPN client from the FortiGate with accounting request messages.

## Configure the FortiGate

### To configure the FortiGate in the CLI:

1. Create a Fortinet Single Sign-On Agent fabric connector:

```
config user fsso
    edit "AD_CollectAgent"
        set server "172.16.200.60"
        set password 123456
    next
end
```

**2. Add the RADIUS server:**

```
config user radius
  edit "rad150"
    set server "172.16.200.150"
    set secret 123456
    set acct-interim-interval 600
    config accounting-server
      edit 1
        set status enable
        set server "172.16.200.60"
        set secret 123456
      next
    end
  next
end
```

**3. Create a user group for the RADIUS server:**

```
config user group
  edit "rad_group"
    set member "rad150"
  next
end
```

**4. Create user groups for each of the FSSO groups:**

```
config user group
  edit "fsso_group1"
    set group-type fsso-service
    set member "CN=PC_GROUP1,OU=TESTING,DC=FSSO-QA,DC=COM"
  next
  edit "fsso_group2"
    set group-type fsso-service
    set member "CN=PC_GROUP2,OU=TESTING,DC=FSSO-QA,DC=COM"
  next
end
```

**5. Create an SSL VPN portal and assign the RADIUS user group to it:**

```
config vpn ssl web portal
  edit "testportal"
    set tunnel-mode enable
    set ipv6-tunnel-mode enable
    set web-mode enable
    ...
  next
end
config vpn ssl settings
  ...
  set default-portal "full-access"
  config authentication-rule
    edit 1
      set groups "rad_group"
      set portal "testportal"
    next
  end
end
```

**6. Create firewall addresses:**

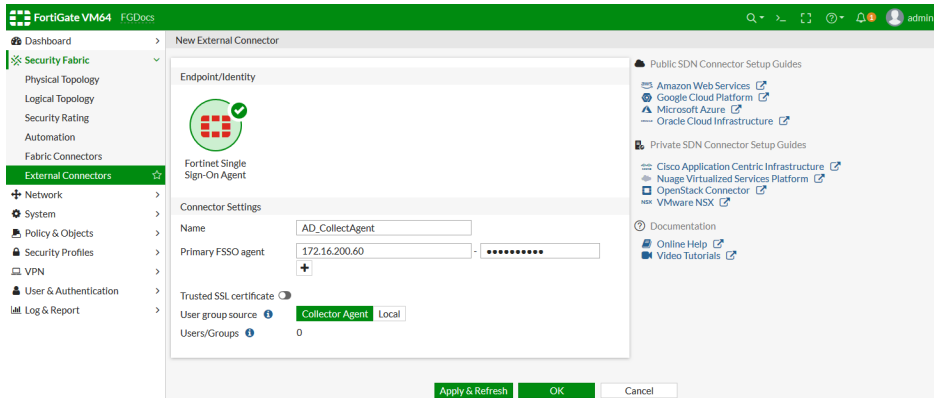
```
config firewall address
  edit "none"
    set subnet 0.0.0.0 255.255.255.255
  next
  edit "pc4"
    set subnet 172.16.200.44 255.255.255.255
  next
  edit "pc5"
    set subnet 172.16.200.55 255.255.255.255
  next
end
```

**7. Create one dummy policy for authentication only, and two normal policies for authorization:**

```
config firewall policy
  edit 1
    set name "sslvpn_authentication"
    set srcintf "ssl.vdom1"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "none"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set groups "rad_group"
    set nat enable
  next
  edit 3
    set name "sslvpn_authorization1"
    set srcintf "ssl.vdom1"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "pc4"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set groups "fsso_group1"
    set nat enable
  next
  edit 4
    set name "sslvpn_authorization2"
    set srcintf "ssl.vdom1"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "pc5"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set groups "fsso_group2"
    set nat enable
  next
end
```

### To create an FSSO agent fabric connector in the GUI:

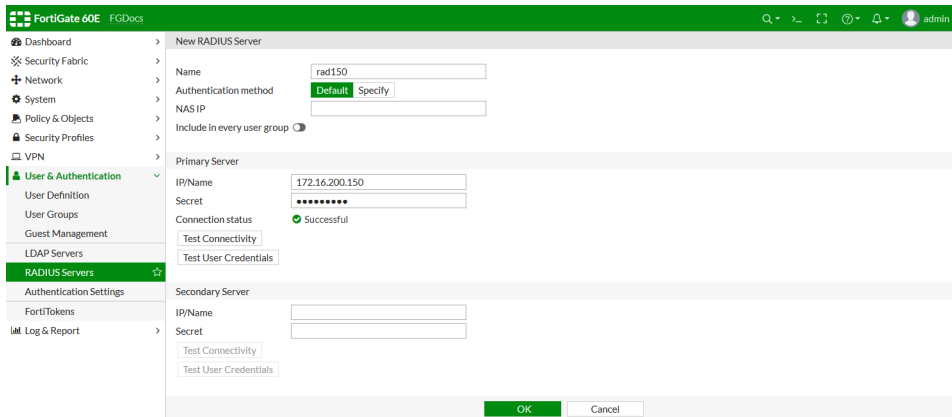
1. Go to *Security Fabric > External Connectors*.
2. Click *Create New*.
3. Click *Fortinet Single Sign-On Agent*.
4. Enter the name and *Primary FSSO agent* information.



5. Click *Apply & Refresh*.  
The FSSO groups are retrieved from the collector agent.

### To add the RADIUS server in the GUI:

1. Go to *User & Authentication > RADIUS Servers*.
2. Click *Create New*.
3. Enter a name for the server.
4. Enter the *IP/Name* and *Secret* for the primary server.
5. Click *Test Connectivity* to ensure that there is a successful connection.



6. Click *OK*.
7. Configure an accounting server with the following CLI command:

```
config user radius
edit rad150
set acct-interim-interval 600
config accounting-server
edit 1
set status enable
```

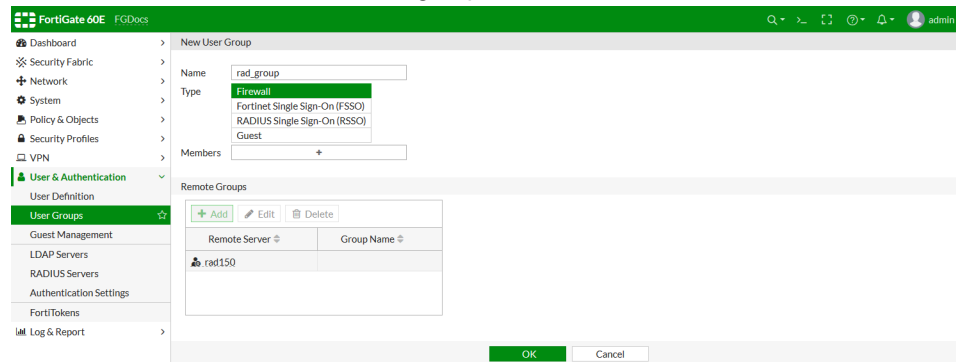
```

        set server 172.16.200.60
        set secret *****
    next
end
next
end

```

### To create a user group for the RADIUS server in the GUI:

1. Go to *User & Authentication > User Groups*.
2. Click *Create New*.
3. Enter a name for the group and set the *Type* to *Firewall*.
4. Add the RADIUS server as a remote group.

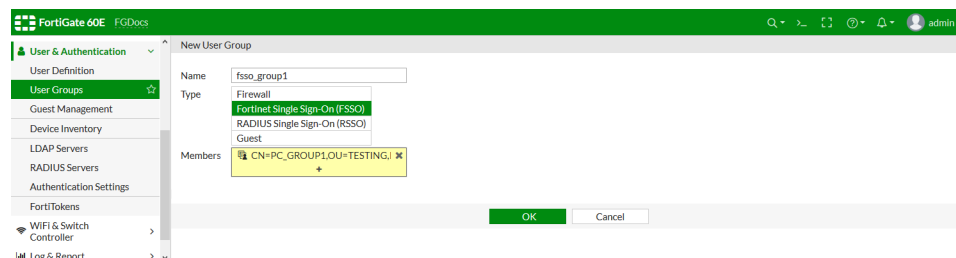


5. Click *OK*.

### To create user groups for each of the FSSO groups in the GUI:

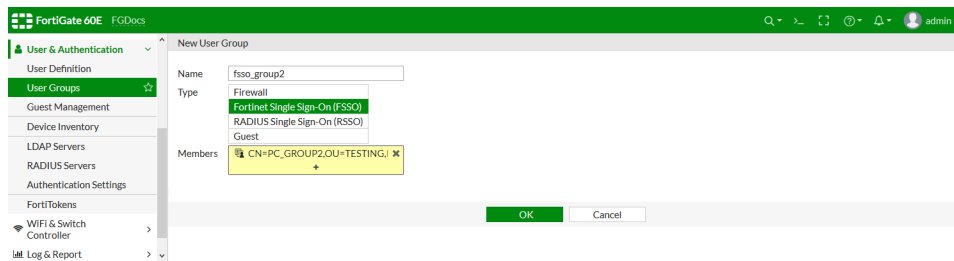
1. Go to *User & Authentication > User Groups*.
2. Click *Create New*.
3. Enter a name for the group and set the *Type* to *Fortinet Single Sign-On (FSSO)*.
4. Add PC\_GROUP1 as a member:

CN=PC\_GROUP1, OU=TESTING, DC=FSSO-QA, DC=COM



5. Click *OK*.
6. Add a second user group with PC\_GROUP2 as a member:

CN=PC\_GROUP2, OU=TESTING, DC=FSSO-QA, DC=COM



7. Click **OK**.

**To create an SSL VPN portal and assign the RADIUS user group to it in the GUI:**

1. Go to **VPN > SSL-VPN Portals**.
2. Click **Create New**.
3. Configure the portal, then click **OK**.
4. Go to **VPN > SSL-VPN Settings**.
5. Configure the required settings.
6. Create an **Authentication/Portal Mapping** table entry:
  - a. Click **Create New**.
  - b. Set **User/Groups** to **rad\_group**.
  - c. Set **Portal** to **testportal**.
  - d. Click **OK**.
7. Click **OK**.

**To create policies for authentication and authorization in the GUI:**

1. Go to **Policy & Object > Firewall Policy**.
2. Configure a dummy policy for authentication. Set the destination to *none* so that traffic is not allowed through the FortiGate, and add **rad\_group** as a source.
3. Configure two authorization policies, with the FSSO groups as sources.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
1	sslvpn_authentication	sslvdsm1	port1	all rad_group	none	always	ALL	ACCEPT	Enabled	SSL no-inspection	All
3	sslvpn_authorization1	sslvdsm1	port1	all fso_group1	pc4	always	ALL	ACCEPT	Enabled	SSL no-inspection	All
4	sslvpn_authorization2	sslvdsm1	port1	all fso_group2	pc5	always	ALL	ACCEPT	Enabled	SSL no-inspection	All
0	Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled

## Confirmation

On *Client 1*, log in to FortiClient using *user142*. Traffic can go to *pc4* (172.16.200.44), but cannot go to *pc5* (172.16.200.55).

On *Client 2*, log in to FortiClient using *user143*. Traffic can go to *pc5* (172.16.200.55), but cannot go to *pc4* (172.16.200.44).

On the FortiGate, check the authenticated users list and the SSL VPN status:

```
# diagnose firewall auth list

10.212.134.200, USER142
  type: fsso, id: 0, duration: 173, idled: 173
  server: AD_CollectAgent
  packets: in 0 out 0, bytes: in 0 out 0
  user_id: 16777229
  group_id: 3 33554434
  group_name: fsso_group1 CN=PC_GROUP1,OU=TESTING,DC=FSSO-QA,DC=COM

10.212.134.200, user142
  type: fw, id: 0, duration: 174, idled: 174
  expire: 259026, allow-idle: 259200
  flag(80): sslvpn
  server: rad150
  packets: in 0 out 0, bytes: in 0 out 0
  group_id: 4
  group_name: rad_group

10.212.134.201, USER143
  type: fsso, id: 0, duration: 78, idled: 78
  server: AD_CollectAgent
  packets: in 0 out 0, bytes: in 0 out 0
  group_id: 1 33554435
  group_name: fsso_group2 CN=PC_GROUP2,OU=TESTING,DC=FSSO-QA,DC=COM

10.212.134.201, user143
  type: fw, id: 0, duration: 79, idled: 79
  expire: 259121, allow-idle: 259200
  flag(80): sslvpn
  server: rad150
  packets: in 0 out 0, bytes: in 0 out 0
  group_id: 4
  group_name: rad_group

----- 4 listed, 0 filtered -----

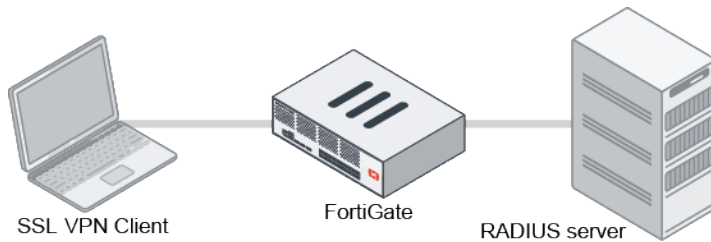
# get vpn ssl monitor
SSL VPN Login Users:
  Index   User      Auth Type      Timeout      From      HTTP in/out  HTTPS in/out
  0       user142    2(1)          600          10.1.100.145 0/0          0/0
  1       user143    2(1)          592          10.1.100.254 0/0          0/0

SSL VPN sessions:
  Index   User      Source IP      Duration      I/O Bytes      Tunnel/Dest IP
  0       user142    10.1.100.145   104           32190/16480     10.212.134.200
  1       user143    10.1.100.254   11            4007/4966       10.212.134.201
```

## NAS-IP support per SSL VPN realm

For RADIUS authentication and authorization, the RADIUS client (the FortiGate) passes the username, password, and NAS-IP to the RADIUS server in its access request. The RADIUS server authenticates and authorizes based on this information. Each RADIUS server can be configured with multiple NAS-IPs for authenticating different groups and NAS clients.

On the FortiGate, configuring the NAS-IP in the realm settings overrides the RADIUS server setting, allowing multiple NAS-IPs to be mapped to the same RADIUS server.



In this example, the user wants to present one FortiGate VDOM with different NAS-IPs to a single RADIUS server based on specific rules.

### To configure the SSL VPN to use the NAS-IP in the realm settings:

1. Configure a RADIUS user and add it to a group:

```

config user radius
  edit "fac150"
    set server "172.16.200.150"
    set secret *****
    set nas-ip 172.16.200.2
    config accounting-server
      edit 1
        set status enable
        set server "172.16.200.150"
        set secret *****
      next
    end
  next
end
config user group
  edit "radgrp"
    set member "fac150"
  next
end

```

2. Configure a realm for the user with a different NAS-IP:

```

config vpn ssl web realm
  edit "realm1"
    set login-page '.....'
    set radius-server "fac150"
    set nas-ip 10.1.100.2
  next
end

```

3. Configure SSL VPN with an authentication rule that includes the user group and the realm:

```

config vpn ssl settings
  ...
  config authentication-rule
    edit 1
      set groupd "radgrp"
      set portal "testportal1"
      set realm "realm1"
    end
  end
end

```



```

    next
  end
end

```

#### 4. Create a firewall policy:

```

config firewall policy
  edit 1
    set name "sslvpn1"
    ...
    set srcintf "ssl.vdom1"
    set groups "radgrp"
  next
end

```

Because the RADIUS server and NAS-IP are specified in realm1, its NAS-IP is used for authentication.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.200.2	172.16.200.150	RADIUS	244	Access-Request id=53
2	0.023546	172.16.200.150	172.16.200.2	RADIUS	258	Access-Accept id=53
3	0.023898	172.16.200.2	172.16.200.150	RADIUS	167	Accounting-Request id=54
4	0.024161	172.16.200.150	172.16.200.2	RADIUS	62	Accounting-Response id=54
5	6.273833	172.16.200.2	172.16.200.150	RADIUS	179	Accounting-Request id=55
6	6.274259	172.16.200.150	172.16.200.2	RADIUS	62	Accounting-Response id=55
7	21.926931	172.16.200.2	172.16.200.44	RADIUS	179	Access-Request id=56
8	21.927204	172.16.200.44	172.16.200.2	RADIUS	95	Access-Accept id=56
9	333.703964	172.16.200.2	172.16.200.150	RADIUS	244	Access-Request id=57
10	333.727478	172.16.200.150	172.16.200.2	RADIUS	258	Access-Accept id=57
11	333.727796	172.16.200.2	172.16.200.150	RADIUS	167	Accounting-Request id=58
12	333.728064	172.16.200.150	172.16.200.2	RADIUS	62	Accounting-Response id=58
13	339.945653	172.16.200.2	172.16.200.150	RADIUS	179	Accounting-Request id=59
14	339.945964	172.16.200.150	172.16.200.2	RADIUS	62	Accounting-Response id=59

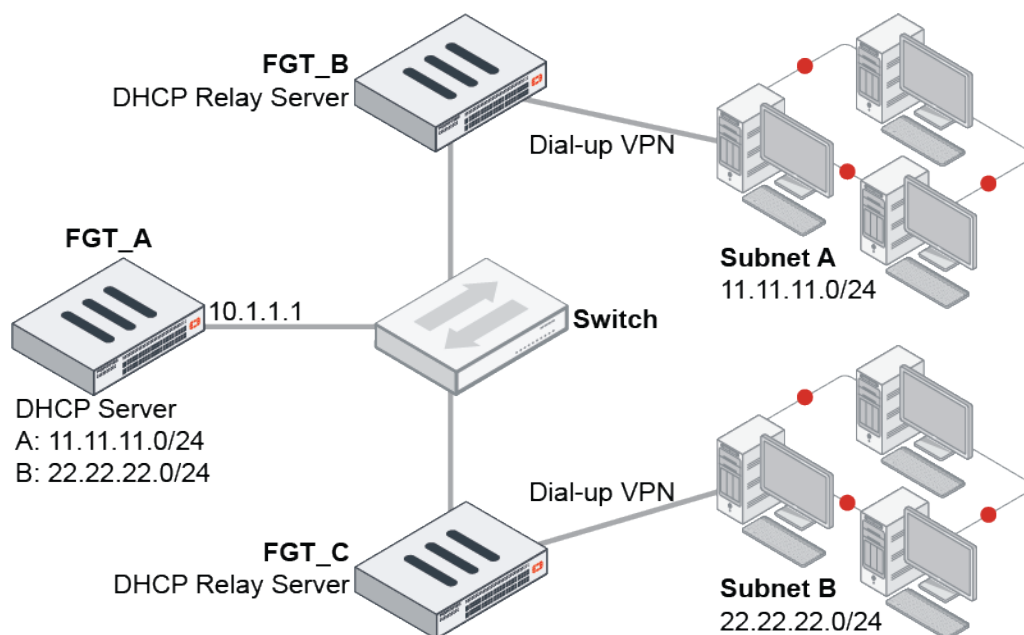
**RADIUS Protocol**  
 Code: Access-Request (1)  
 Packet Identifier: 0x35 (53)  
 Length: 202  
 Authenticator: 4e08c9af837dc2cd217e21f4fda81cc  
 [The response to this request is in frame 2]  
 Attribute Value Pairs  
 > AVP: t=NAS-Identifier(32) l=18 val=F64H1E5819900552  
 > AVP: t=User-Name(1) l=6 val=fac3  
 > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)  
 > AVP: t=Vendor-Specific(26) l=24 vnd=Microsoft(311)  
 > AVP: t=NAS-IP-Address(4) l=6 val=10.1.100.2

## Support defining gateway IP addresses in IPsec with mode-config and DHCP

For an IPsec tunnel, the gateway IP address (giaddr) can be defined on a DHCP relay agent. Both IPv4 and IPv6 addresses are supported. An IPsec tunnel with mode-config and DHCP relay cannot specify a DHCP subnet range to the DHCP server.

The DHCP server assigns an IP address based on the giaddr set on the IPsec phase1 interface and sends an offer to this subnet. The DHCP server must have a route to the specified subnet giaddr.

## Example



To define the gateway IP address on the DHCP relay server:

1. Configure the VPN IPsec phase1 interface:

```
config vpn ipsec phase1-interface
  edit "ipv4"
    set type dynamic
    set interface "port2"
    set peertype any
    set net-device disable
    set mode-cfg enable
    set proposal des-md5 des-sha1
    set dpd on-idle
    set dhgrp 5
    set assign-ip-from dhcp
    set dhcp-ra-giaddr 11.11.11.1
    set psksecret *****
    set dpd-retryinterval 60
  next
end
```

IPv6 could also be configured:

```
config vpn ipsec phase1-interface
  edit "ipv6"
    set type dynamic
    set interface "port2"
    set peertype any
    set net-device disable
    set mode-cfg enable
    set proposal des-md5 des-sha1
    set dpd on-idle
```

```
        set dhgrp 5
        set assign-ip-from dhcp
        set dhcp6-ra-linkaddr 2000:11:11:11::1
        set psksecret *****
        set dpd-retryinterval 60
    next
end
```

2. Enable DHCP proxy and configure the DHCP server IP address:

```
config system settings
    set dhcp-proxy enable
    set dhcp-server-ip "10.1.1.1"
end
```

3. Repeat the above steps for FGT\_C and subnet B.

## Provision SSL VPN users in FortiClient Mobile with an email or SMS message - 6.4.2



This feature requires FortiClient Mobile for Android or iOS version 6.4.2 or later

---

A QR code and URI can be sent to users in an email or SMS message, allowing them to automatically provision SSL VPN in the FortiClient Mobile app for Android or iOS.

## Configure DSCP for IPsec tunnels - 6.4.3

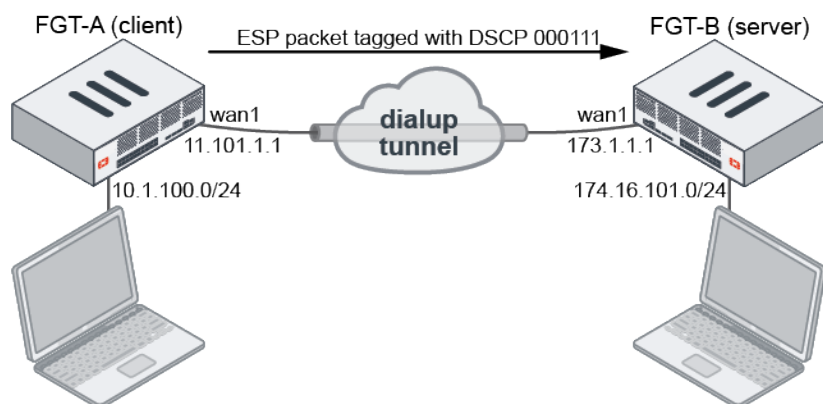
Configuring the differentiated services (DiffServ) code in phase2 of an IPsec tunnel allows the tag to be applied to the Encapsulating Security Payload (ESP) packet.

- If `diffserv` is disabled in the IPsec phase2 configuration, then the ESP packets' DSCP value is copied from the inner IP packet DSCP.
- If `diffserv` is enabled in the IPsec phase2 configuration, then ESP packets' DSCP value is set to the configured value.



Offloading traffic to the NPU must be disabled for the tunnel.

---



In this example, NPU offloading is disabled, diffserv is enabled, and the diffserv code is set to 000111 on FGT-A. Only one side of the tunnel needs to have diffserv enabled.

### To configure IPsec on FGT-A:

#### 1. Configure the phase1-interface:

```
config vpn ipsec phase1-interface
  edit "s2s"
    set interface "wan1"
    set peertype any
    set net-device disable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set npu-offload disable
    set dhgrp 14 5
    set wizard-type static-fortigate
    set remote-gw 173.1.1.1
    set psksecret *****
  next
end
```

#### 2. Configure the phase2-interface:

```
config vpn ipsec phase2-interface
  edit "s2s"
    set phase1name "s2s"
    set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
    aes256gcm chacha20poly1305
    set dhgrp 14 5
    set diffserv enable
    set diffservcode 000111
    set src-addr-type name
    set dst-addr-type name
    set src-name "s2s_local"
    set dst-name "s2s_remote"
  next
end
```

#### 3. Check the state of the IPsec tunnel:

```
FGT-A # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
```

```
-----
```

```

name=s2s ver=1 serial=1 11.101.1.1:0->173.1.1.1:0 dst_mtu=1500
bound_if=17 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/512 options[0200]=frag-rfc
run_state=0 accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=11 ilast=12 olast=2978 ad=/0
stat: rxp=4 txp=4 rxb=608 txb=336
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=s2s proto=0 sa=1 ref=2 serial=2 dscp
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:174.16.101.0/255.255.255.0:0
SA: ref=3 options=110226 type=00 soft=0 mtu=1438 expire=39916/0B replaywin=2048
seqno=5 esn=0 replaywin_lastseq=00000005 itn=0 qat=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=42899/43200
dec: spi=a41f202e esp=aes key=16 8a02875b80b884d961af227fe8b5cdee
ah=sha1 key=20 fc9760b79e79dbb0ef630ec0c5dca74777976208
enc: spi=431bce1e esp=aes key=16 851117af24212da89e466d8bea9632bb
ah=sha1 key=20 0807cc0af2dc4ea049a6b1a4af410ccc71e2156d
dec:pkts/bytes=4/336, enc:pkts/bytes=4/608
npu_flag=00 npu_rgwy=173.1.1.1 npu_lgwy=11.101.1.1 npu_selid=1 dec_npuid=0 enc_npuid=0
run_tally=1

```

#### 4. Use a packet analyzer, or sniffer, to check the ESP packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	11.101.1.1	173.1.1.1	ESP	166	ESP (SPI=0x431bce1e)
2	0.000341	173.1.1.1	11.101.1.1	ESP	166	ESP (SPI=0xa41f202e)
3	1.000361	11.101.1.1	173.1.1.1	ESP	166	ESP (SPI=0x431bce1e)
4	1.001073	173.1.1.1	11.101.1.1	ESP	166	ESP (SPI=0xa41f202e)
5	1.999801	11.101.1.1	173.1.1.1	ESP	166	ESP (SPI=0x431bce1e)
6	2.000513	173.1.1.1	11.101.1.1	ESP	166	ESP (SPI=0xa41f202e)
7	3.000212	11.101.1.1	173.1.1.1	ESP	166	ESP (SPI=0x431bce1e)

> Frame 1: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits)

> Ethernet II, Src: Fortinet\_12:6a:24 (70:4c:a5:12:6a:24), Dst: Fortinet\_eb:c8:82 (08:5b:0e:eb:c8:82)

▼ Internet Protocol Version 4, Src: 11.101.1.1, Dst: 173.1.1.1

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

▼ Differentiated Services Field: 0x1c (DSCP: Unknown, ECT: Not-ECT)

0001 11.. = Differentiated Services Codepoint: Unknown (7)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 152

Identification: 0x0500 (1280)

> Flags: 0x0000

Fragment offset: 0

Time to live: 62

Protocol: Encap Security Payload (50)

Header checksum: 0xbcb0 [validation disabled]

[Header checksum status: Unverified]

Source: 11.101.1.1

Destination: 173.1.1.1

> Encapsulating Security Payload

# User and authentication

This section includes information about user and authentication related new features:

- [Authentication on page 344](#)

## Authentication

This section includes information about authentication related new features:

- [SAML SP for VPN authentication on page 344](#)
- [Support for Okta RADIUS attributes filter-Id and class on page 347](#)
- [Multiple LDAP servers in Kerberos keytabs and agentless NTLM domain controllers 6.4.3 on page 349](#)
- [Traffic shaping based on dynamic RADIUS VSAs 6.4.6 on page 350](#)

## SAML SP for VPN authentication

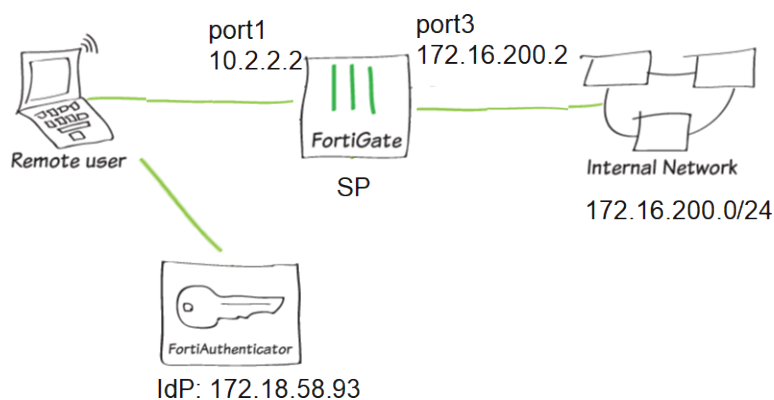
When you configure a FortiGate as a service provider (SP), you can create an authentication profile that uses SAML for both firewall and SSL VPN web portal authentication. Once the firewall is authenticated, entering SAML credentials is not required for SSL VPN web portal authentication.



You must use the identity provider's (IdP) remote certificate on the SPs.

---

The following example uses a FortiGate as an SP and FortiAuthenticator as the IdP server:



**To configure firewall authentication:****1. Configure the FortiGate SP to be a SAML user:**

```
config user saml
  edit "fac-firewall"
    set entity-id "http://10.2.2.2:1000/saml/metadata/"
    set single-sign-on-url "https://10.2.2.2:1003/saml/login/"
    set single-logout-url "https://10.2.2.2:1003/saml/logout/"
    set idp-entity-id "http://172.18.58.93:443/saml-idp/bbbbbbb/metadata/"
    set idp-single-sign-on-url "https://172.18.58.93:443/saml-idp/bbbbbbb/login/"
    set idp-single-logout-url "https://172.18.58.93:443/saml-idp/bbbbbbb/logout/"
    set idp-cert "REMOTE_Cert_3"
    set user-name "username"
    set group-name "group"
  next
end
```

**2. Add the SAML user to the user group (optionally, you can configure group matching):**

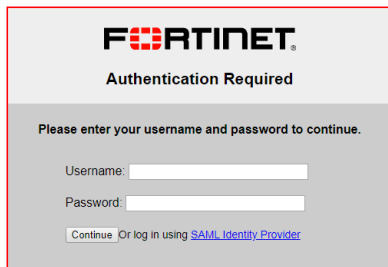
```
config user group
  edit "saml_firewall"
    set member "fac-firewall"
    config match
      edit 1
        set server-name "fac-firewall"
        set group-name "user_group1"
      next
    end
  next
end
```

**3. Add the SAML user group to a firewall policy:**

```
config firewall policy
  edit 2
    set srcintf "port3"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "pc4"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set fsso disable
    set groups "saml_firewall" "group_local"
    set users "first"
    set nat enable
  next
end
```

**4. Configure the FortiAuthenticator IdP as needed.**

5. Run HTTP/HTTPS authentication for a remote user. The SAML login page appears:



The image shows a web page titled "FORTINET Authentication Required". Below the title, it says "Please enter your username and password to continue." There are two input fields: "Username:" and "Password:". Below the password field, there is a link that says "Continue" followed by "Or log in using [SAML Identity Provider](#)".

### To configure SSL VPN web portal authentication:

1. Configure the FortiGate SP to be a SAML user:

```
config user saml
  edit "fac-sslvpn"
    set entity-id "https://10.2.2.2:10443/remote/saml/metadata/"
    set single-sign-on-url "https://10.2.2.2:10443/remote/saml/login/"
    set single-logout-url "https://10.2.2.2:10443/remote/saml/logout/"
    set idp-entity-id "http://172.18.58.93:443/saml-idp/sss/sss/metadata/"
    set idp-single-sign-on-url "https://172.18.58.93:443/saml-idp/sss/sss/login/"
    set idp-single-logout-url "https://172.18.58.93:443/saml-idp/sss/sss/logout/"
    set idp-cert "REMOTE_Cert_3"
    set user-name "username"
  next
end
```

2. Add the SAML user to the user group (group matching may also be configured):

```
config user group
  edit "saml_sslvpn"
    set member "fac-sslvpn"
  next
end
```

3. Configure SSL VPN:

```
config vpn ssl settings
  set servercert "Fortinet_Factory"
  set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
  set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
  set source-interface "port3"
  set source-address "all"
  set source-address6 "all"
  set default-portal "full-access"
  config authentication-rule
    edit 1
      set groups "saml_sslvpn"
      set portal "web-access"
    next
  end
end
```

4. Add the SAML user group to a firewall policy:

```
config firewall policy
  edit 8
```

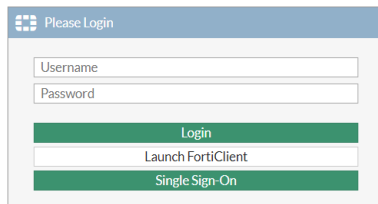


```

set srcintf "ssl.vdom1"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set groups "local" "saml_sslvpn"
set nat enable
next
end

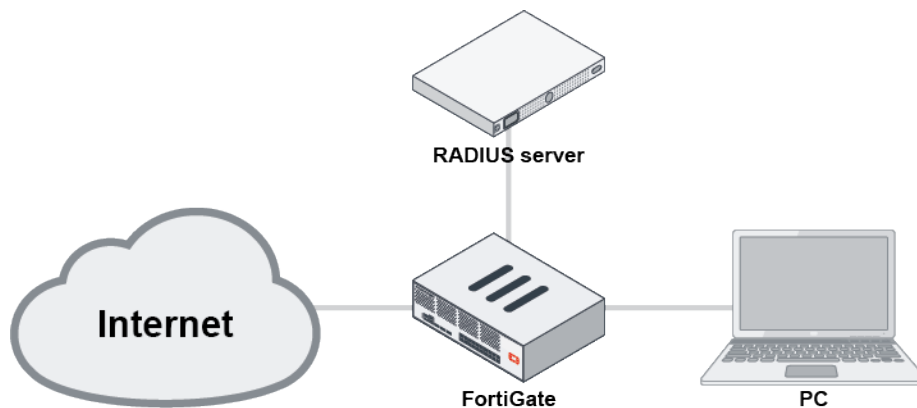
```

5. Configure the FortiAuthenticator IdP as needed.
6. Run SSL VPN web mode authentication for a remote user. The SAML login page appears:



## Support for Okta RADIUS attributes filter-Id and class

This feature adds support for RADIUS user group membership information that is returned in the filter-Id (11) and class (25) attributes in RADIUS Access-Accept messages. The group membership information can be used for group matching in FortiGate user groups in firewall policies and for FortiGate wildcard administrators with remote RADIUS authentication.



In this example, a FortiAuthenticator is used as the RADIUS server. A local RADIUS user on the FortiAuthenticator is configured with two groups in the filter-Id attribute: *okta-group1* and *okta-group2*.

**To create the RADIUS user and set the attribute type to override group information:**

```

config user radius
edit "FAC193"
set server "10.1.100.189"
set secret *****
set group-override-attr-type filter-Id

```

```

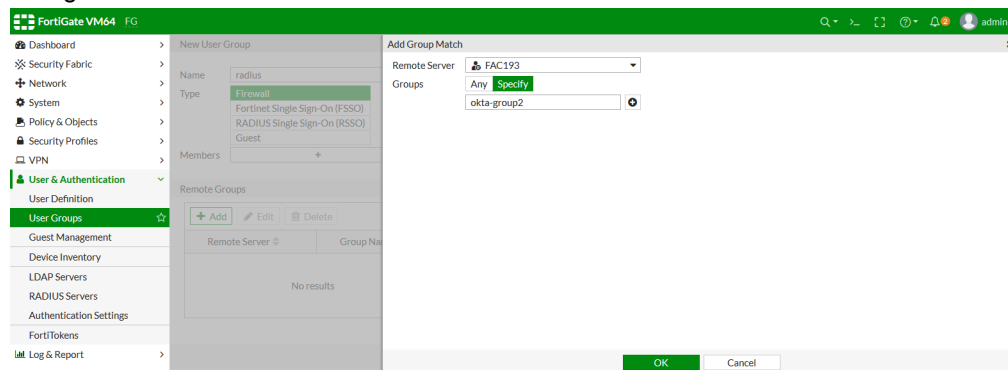
next
end

```

FortiOS will only use the configured filter-Id attribute, even if the RADIUS server sends group names in both class and filter-id attributes. To return group membership information from the class attribute instead, set `group-override-attr-type` to `class`.

### To configure group match in the user group:

1. Go to *User & Authentication > User Groups*.
2. Click *Create New*.
3. Enter a name for the group, and set *Type* to *Firewall*.
4. In the *Remote Groups* table, click *Add*.
5. Set *Remote Server* to the just created RADIUS server, *FAC193*.
6. Set *Groups* to *Specify*, and enter the group name, *okta-group2*. The string must match the group name configured on the RADIUS server for the filter-Id attribute.

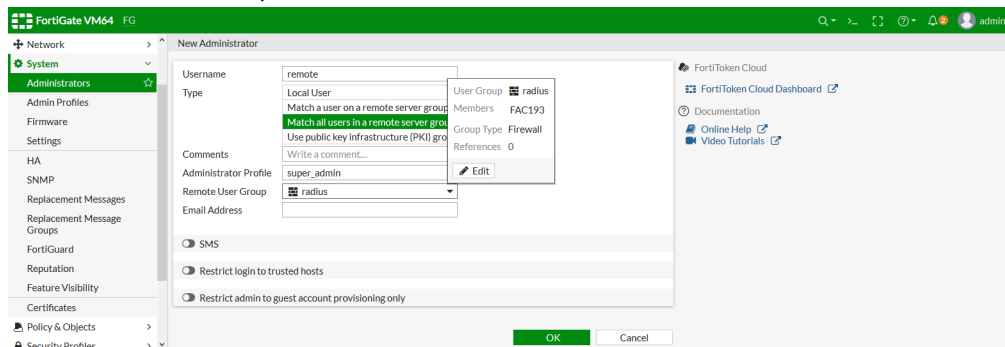


7. Click *OK*.  
The remote server is added to the *Remote Groups* table.
8. Click *OK*.
9. Add the new user group to a firewall policy and generate traffic on the client PC that requires firewall authentication, such as connecting to an external web server.
10. After authentication, on the FortiGate, verify that traffic is authorized in the traffic log:
  - a. Go to *Log & Report > Forward Traffic*.
  - b. Verify that the traffic was authorized.

### To use the remote user group with group match in a system wildcard administrator configuration:

1. Go to *System > Administrators*.
2. Edit an existing administrator, or create a new one.
3. Set *Type* to *Match all users in a remote server group*.

#### 4. Set *Remote User Group* to the remote server.



#### 5. Configure the remaining settings as required.

#### 6. Click **OK**.

#### 7. Log in to the FortiGate using the remote user credentials on the RADIUS server.

If the correct group name is returned in the filter-Id attribute, administrative access is allowed.

## Multiple LDAP servers in Kerberos keytabs and agentless NTLM domain controllers

- 6.4.3

Multiple LDAP servers can be configured in Kerberos keytabs and agentless NTLM domain controllers for multi-forest deployments.

### To use multiple LDAP servers in Kerberos keytabs and agentless NTLM domain controllers:

#### 1. Add multiple LDAP servers:

```
config user ldap
    edit "ldap-kerberos"
        set server "172.16.200.98"
        set cnid "cn"
        set dn "dc=fortinetqa,dc=local"
        set type regular
        set username "CN=root,CN=Users,DC=fortinetqa,DC=local"
        set password xxxxxxxxxx
    next
    edit "ldap-two"
        set server "172.16.106.128"
        set cnid "cn"
        set dn "OU=Testing,DC=ad864r2,DC=com"
        set type regular
        set username "cn=Testadmin,cn=users,dc=AD864R2,dc=com"
        set password xxxxxxxxxx
    next
end
```

#### 2. Configure a Kerberos keytab entry that uses both LDAP servers:

```
config user krb-keytab
    edit "http_service"
        set pac-data disable
        set principal "HTTP/FGT.FORTINETQA.LOCAL@FORTINETQA.LOCAL"
        set ldap-server "ldap-kerberos" "ldap-two"
```

```

        set keytab xxxxxxxxx
    next
end

```

### 3. Configure a domain controller that uses both LDAP servers:

```

config user domain-controller
    edit "dc1"
        set ip-address 172.16.200.98
        set ldap-server "ldap-two" "ldap-kerberos"
    next
end

```

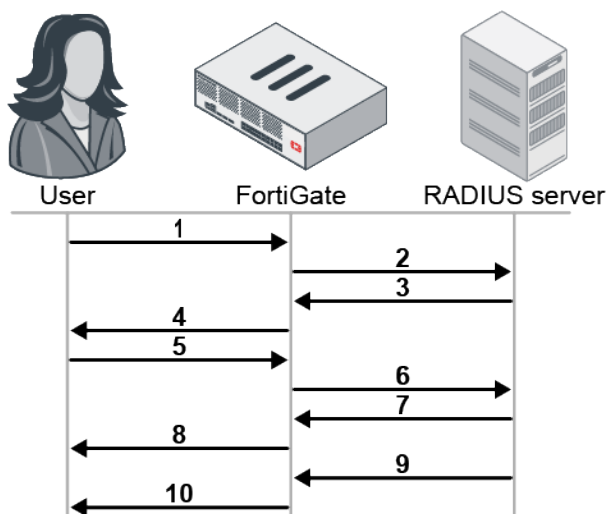
## Traffic shaping based on dynamic RADIUS VSAs - 6.4.6

A FortiGate can use the WISPr-Bandwidth-Max-Down and WISPr-Bandwidth-Max-Up dynamic RADIUS VSAs (vendor-specific attributes) to control the traffic rates permitted for a certain device. The FortiGate can apply different traffic shaping to different users who authenticate with RADIUS based on the returned RADIUS VSA values. When the same user logs in from an additional device, the RADIUS server will send a CoA (change of authorization) message to update the bandwidth values to  $1/N$  of the total values, where  $N$  is the number of logged in devices from the same user.



This feature is not supported on NP hardware. NP offloading is automatically disabled on the policy if this feature is enabled.

When a user logs in to two devices through RADIUS authentication. The authentication and authorization flow is as follows:

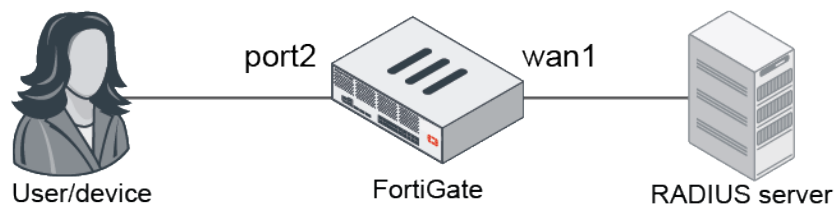


1. The user logs in to a device and the authentication is sent to the FortiGate.
2. The FortiGate sends the Access-Request message to the RADIUS server.
3. The RADIUS server sends the Access-Accept message to the FortiGate. The server also returns the WISPr-Bandwidth-Max-Up and WISPr-Bandwidth-Max-Down VSAs.
4. Based on the VSA values, the FortiGate applies traffic shaping for the upload and download speeds based on its IP.
5. The user logs in to a second device and the authentication is sent to the FortiGate.
6. The FortiGate sends the Access-Request message to the RADIUS server.

7. The RADIUS server sends the Access-Accept message to the FortiGate. The server also returns the WISPr-Bandwidth-Max-Up and WISPr-Bandwidth-Max-Down VSAs at half the value from the first device.
8. Based on the VSA values, the FortiGate applies traffic shaping for the upload and download speeds on the second device based on its IP.
9. The RADIUS server sends a CoA message and returns WISPr-Bandwidth-Max-Up and WISPr-Bandwidth-Max-Down VSAs for the first device at half the value.
10. Based on the VSA values, the FortiGate updates traffic shaping for the upload and download speeds on the first device based on its IP.

## Example

In this example, the FortiGate is configured to dynamically shape user traffic based on the WISPr-Bandwidth-Max-Up and WISPr-Bandwidth-Max-Down VSAs returned by the RADIUS server when the user logs in through firewall authentication.



### To configure traffic shaping based on dynamic RADIUS VSAs:

1. Configure the RADIUS server users file to identify WISPr-Bandwidth-Max-Up and WISPr-Bandwidth-Max-Down:



The WISPr-Bandwidth is measured in bps, and the FortiOS dynamic shaper is measured in Bps.

```

WISPr-Bandwidth-Max-Up = 1004857,
WISPr-Bandwidth-Max-Down = 504857,
  
```

2. In FortiOS, configure the RADIUS server:

```

config user radius
  edit "rad1"
    set server "172.16.200.44"
    set secret *****
    set radius-coa enable
    set acct-all-servers enable
    config accounting-server
      edit 1
        set status enable
        set server "172.16.200.44"
        set secret *****
      next
    end
  next
end
  
```

**3. Configure the RADIUS user group:**

```
config user group
    edit "group_radius"
        set member "rad1"
    next
end
```

**4. Configure the firewall policy with dynamic shaping and the RADIUS group:**

```
config firewall policy
    edit 2
        set srcintf "port2"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all6"
        set dstaddr6 "all6"
        set action accept
        set schedule "always"
        set service "ALL"
        set dynamic-shaping enable
        set groups "group_radius"
        set nat enable
    next
end
```

## Verification

After a client PC is authenticated by the RADIUS server, dynamic shaping is applied to the client based on the IP address.

Use the following commands to monitor the dynamic shaper:

```
# diagnose firewall shaper dynamic-shaper stats
# diagnose firewall shaper dynamic-shaper list {ip | ipv6 | user} <address or username>
```

### Use case 1

User1 is paying for rate plan A that limits their maximum bandwidth to 10 Mbps download and 5 Mbps upload. User2 is paying for rate plan B that limits their maximum bandwidth to 5 Mbps download and 5 Mbps upload. The speeds in both plans are provided by best effort, so there is no guaranteed minimum bandwidth.

User1 logs in to pc1 with RADIUS authentication and IP-based dynamic shaping is applied. User2 logs in to pc2 with RADIUS authentication and IP-based dynamic shaping is applied.

**To verify the dynamic shaping:****1. On pc1, verify the bandwidth and transfer speed:**

```
root@pc1:~# iperf -c 172.16.200.44 -u -t 25 -b 20M
-----
Client connecting to 172.16.200.44, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 208 KByte (default)
```

```

-----
[ 3] local 10.1.100.11 port 50510 connected with 172.16.200.44 port 5001
[ ID] Interval      Transfer      Bandwidth
[ 3] 0.0-25.0 sec  59.6 MBytes  20.0 Mbits/sec
[ 3] Sent 42518 datagrams
[ 3] Server Report:
[ 3] 0.0-25.3 sec  30.1 MBytes  9.99 Mbits/sec  15.651 ms 21058/42518 (50%)

```

## 2. On pc2, verify the bandwidth and transfer speed:

```

root@pc2:~# iperf -c 172.16.200.44 -u -t 25 -b 20M
-----
Client connecting to 172.16.200.44, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 208 KByte (default)
-----
[ 3] local 10.1.100.22 port 52814 connected with 172.16.200.44 port 5001
[ ID] Interval      Transfer      Bandwidth
[ 3] 0.0-25.0 sec  59.6 MBytes  20.0 Mbits/sec
[ 3] Sent 42518 datagrams
[ 3] Server Report:
[ 3] 0.0-25.3 sec  15.1 MBytes  5.03 Mbits/sec  15.652 ms 31710/42514 (75%)

```

## 3. In FortiOS, check the authentication list:

```

# diagnose firewall auth list
10.1.100.11, test-shaper1
    src_mac: **:***:***:***:***:***
    type: fw, id: 0, duration: 38, idled: 16
    expire: 562
    flag(814): hard radius no_idle
    server: rad1
    packets: in 8207 out 3999, bytes: in 12306164 out 226963
    group_id: 3
    group_name: group_radius
10.1.100.22, test-shaper2
    src_mac: **:***:***:***:***:***
    type: fw, id: 0, duration: 24, idled: 24
    expire: 156, max-life: 35976
    flag(814): hard radius no_idle
    server: rad1
    packets: in 0 out 5, bytes: in 0 out 300
    group_id: 3
    group_name: group_radius
----- 2 listed, 0 filtered -----

```

## 4. Check the dynamic shaper list:

```

# diagnose firewall shaper dynamic-shaper list
addr: 10.1.100.11
bandwidth(original/reply): 1250000 Bps/625000 Bps
current bandwidth(original/reply): 1237072 Bps/0 Bps
allow packets(original/reply): 38524/14
allow bytes(original/reply): 55270378/11285
drop packets(original/reply): 10136/0
drop bytes(original/reply): 13516198/0
life: 441
idle: 0/40

```

```

idle time limit: 600 s

addr: 10.1.100.22
bandwidth(original/reply): 625000 Bps/625000 Bps
current bandwidth(original/reply): 622909 Bps/0 Bps
allow packets(original/reply): 3232/3
allow bytes(original/reply): 4841536/243
drop packets(original/reply): 2753/0
drop bytes(original/reply): 4123994/0
life: 10
idle: 0/10
idle time limit: 36000 s

```

## 5. Check the session list:

```

# diagnose sys session list
session info: proto=6 proto_state=05 duration=3 expire=116 timeout=3600 flags=00000004
socktype=4 sockport=10001 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=redir log local may_dirty auth dst-vis f00 dynamic_shaping
statistic(bytes/packets/allow_err): org=0/0/0 reply=638/4/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 185/1
orgin->sink: org pre->post, reply pre->post dev=20->17/17->20 gwy=172.16.200.44/0.0.0.0
hook=pre dir=org act=noop 10.1.100.22:35561->172.16.200.44:80(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.200.44:80->10.1.100.22:35561(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=**:**:**:**:**:** dst_mac=**:**:**:**:**
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=1
serial=0005994d tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x000001 no_offload
no_ofld_reason: redir-to-av auth disabled-by-policy

session info: proto=6 proto_state=05 duration=122 expire=38 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=test-shaper1 auth_server=rad1 state=log may_dirty authed f00 dynamic_shaping acct-ext
statistic(bytes/packets/allow_err): org=383611/6604/1 reply=26382470/17592/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=20->17/17->20 gwy=172.16.200.44/10.2.2.1
hook=post dir=org act=snat 10.1.100.11:54140->172.16.200.44:80(172.16.200.2:54140)
hook=pre dir=reply act=dnat 172.16.200.44:80->172.16.200.2:54140(10.1.100.11:54140)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=**:**:**:**:**:** dst_mac=**:**:**:**:**
misc=0 policy_id=2 auth_info=3 chk_client_info=0 vd=1
serial=000598c5 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x000001 no_offload

```



```
no_ofld_reason: disabled-by-policy
total session 2
```

## 6. Check the policy traffic:

```
# diagnose firewall iprope list 100004
policy index=2 uuid_idx=60 action=accept
flag (8052128): redir auth nat nids_raw master use_src pol_stats
flag2 (4030): fw wssso resolve_sso
flag3 (200000b0): !sp link-local best-route dynamic-shaping
schedule(always)
cos_fwd=255 cos_rev=255
group=00100004 av=00004e20 au=00000003 split=00000000
host=1 chk_client_info=0x1 app_list=0 ips_view=0
misc=0
zone(1): 20 -> zone(1): 17
source(1): 0.0.0.0-255.255.255.255, uuid_idx=32,
dest(1): 0.0.0.0-255.255.255.255, uuid_idx=32,
user group(1): 3
service(1):
[0:0x0:0/(0,65535)->(0,65535)] helper:auto
```

## Use case 2

A user logs in to a device (pc1, 10.1.100.11) and has a maximum bandwidth of 10 Mbps download and 5 Mbps upload. The same user logs in to a second device (pc2, 10.1.100.22) and the RADIUS server sends a CoA request with the WISPr-Bandwidth-Max to pc1. The maximum bandwidth on pc1 changes to 5 Mbps download and 2.5Mbps upload. On pc2, the maximum bandwidth is also 5 Mbps download and 2.5Mbps upload.

When the user logs out from pc1, the RADIUS server sends CoA request with the new WISPr-Bandwidth-Max for pc2. The FortiGate updates the authentication user list and dynamic shaper for pc2. The maximum bandwidth on pc2 changes to 10 Mbps download and 5 Mbps upload.

## To verify the dynamic shaping:

### 1. Check the dynamic shaper list after the user logs in to pc1:

```
# diagnose firewall shaper dynamic-shaper list
addr: 10.1.100.11
bandwidth(original/reply): 1250000 Bps/625000 Bps
current bandwidth(original/reply): 0 Bps/0 Bps
allow packets(original/reply): 0/3
allow bytes(original/reply): 0/243
drop packets(original/reply): 0/0
drop bytes(original/reply): 0/0
life: 491
idle: 4/4
idle time limit: 86400 s
```

### 2. Check the dynamic shaper list after the user logs in to pc2:

```
# diagnose firewall shaper dynamic-shaper list
addr: 10.1.100.11
bandwidth(original/reply): 625000 Bps/312500 Bps
current bandwidth(original/reply): 0 Bps/0 Bps
allow packets(original/reply): 0/0
allow bytes(original/reply): 0/0
```

```
drop packets(original/reply): 0/0
drop bytes(original/reply): 0/0
life: 652
idle: 5/5
idle time limit: 600 s

addr: 10.1.100.22
bandwidth(original/reply): 625000 Bps/312500 Bps
current bandwidth(original/reply): 0 Bps/0 Bps
allow packets(original/reply): 0/3
allow bytes(original/reply): 0/243
drop packets(original/reply): 0/0
drop bytes(original/reply): 0/0
life: 3
idle: 3/3
idle time limit: 86400 s
```

### 3. Check the authentication list:

```
# diagnose firewall auth list
10.1.100.11, test
    src_mac: **:***:***:***:***:***
    type: fw, id: 0, duration: 171, idled: 11
    expire: 589, max-life: 589
    flag(814): hard radius no_idle
    server: rad1
    packets: in 0 out 0, bytes: in 0 out 0
    group_id: 15
    group_name: group_radius
10.1.100.22, test
    src_mac: **:***:***:***:***:***
    type: fw, id: 0, duration: 9, idled: 9
    expire: 86391
    flag(814): hard radius no_idle
    server: rad1
    packets: in 0 out 0, bytes: in 0 out 0
    group_id: 15
    group_name: group_radius
----- 2 listed, 0 filtered -----
```

### 4. Check the dynamic shaper list after the user logs out from pc1:

```
# diagnose firewall shaper dynamic-shaper list
addr: 10.1.100.22
bandwidth(original/reply): 1250000 Bps/625000 Bps
current bandwidth(original/reply): 0 Bps/0 Bps
allow packets(original/reply): 0/0
allow bytes(original/reply): 0/0
drop packets(original/reply): 0/0
drop bytes(original/reply): 0/0
life: 414
idle: 9/9
idle time limit: 600 s
```

### 5. Check the authentication list again:

```
# diagnose firewall auth list
10.1.100.22, test
```

```
src_mac: **:**:**:**:**:**
type: fw, id: 0, duration: 453, idled: 49
expire: 551, max-life: 551
flag(814): hard radius no_idle
server: rad1
packets: in 0 out 0, bytes: in 0 out 0
group_id: 15
group_name: group_radius
----- 1 listed, 0 filtered -----
```

# Secure access

This section includes information about secure access related new features:

- [Wireless on page 358](#)
- [Switch controller on page 433](#)
- [NAC on page 464](#)
- [FortiExtender on page 475](#)

## Wireless

This section includes information about wireless related new features:

- [Wireless IPv6 support on page 358](#)
- [Support for spectrum analysis of FortiAP E models on page 364](#)
- [Increase in maximum number of managed FortiAPs on page 370](#)
- [Even distribution of FortiAP reports on page 371](#)
- [View detailed information for individual WiFi connections on page 375](#)
- [VLAN probe report on page 383](#)
- [FortiAP client load balancing per AP on page 387](#)
- [Layer three ACL configurations for Wireless APs on page 388](#)
- [Maintain radio SSID WLAN IDs on page 390](#)
- [Support for FAP431F and FAP433F on page 392](#)
- [Support logging the signal-to-noise ratio and signal strength per client 6.4.1 on page 396](#)
- [Simplify BLE profiles to support broadcast of FortiAP UUID 6.4.2 on page 398](#)
- [Add ARP profile for wireless controller 6.4.2 on page 401](#)
- [Extend spectrum analysis to support FortiAPs with three radios 6.4.2 on page 403](#)
- [Antenna Rx chain status check and notification 6.4.2 on page 409](#)
- [Standardize wireless health metrics 6.4.2 on page 410](#)
- [FortiAP query to FortiGuard IoT service to determine device details 6.4.2 on page 414](#)
- [Enhance MPSK functionalities for wireless controller 6.4.2 on page 415](#)
- [Adaptive radio architecture support 6.4.3 on page 418](#)
- [Support 802.11v optimized roaming and load balancing 6.4.3 on page 422](#)
- [Support IGMP Snooping \(Wireless\) 6.4.3 on page 424](#)
- [Use FortiGate to register managed FortiAP to FortiCloud 6.4.3 on page 428](#)
- [Add fields for wireless DHCP logs 6.4.3 on page 431](#)
- [Dynamic VLAN assignment using RADIUS attribute string 6.4.6 on page 431](#)

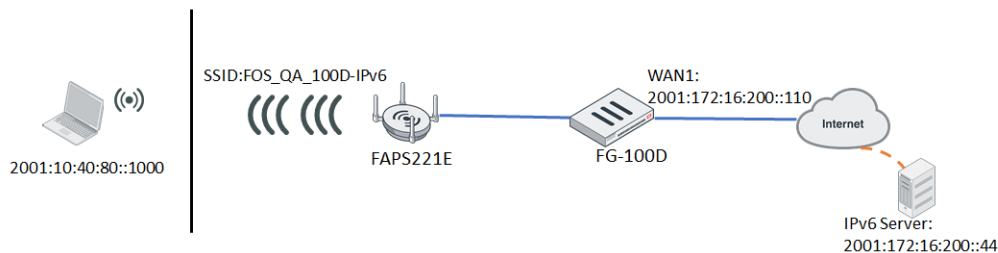
## Wireless IPv6 support

Wireless client IPv6 traffic is supported from both tunnel and local bridge mode SSID:

- [Tunnel mode SSID IPv6 traffic on page 359](#)
- [Local bridge mode SSID IPv6 traffic on page 361](#)
- [CLI commands for IPv6 rules on page 363](#)

## Tunnel mode SSID IPv6 traffic

In the following example, FortiAP S221E is managed by FortiGate 100D and broadcasts tunnel mode SSID:FOS\_QA\_100D-IPv6.



### To configure a WiFi client accessing IPv6 tunnel mode traffic:

#### 1. Create a tunnel mode VAP:

```
config wireless-controller vap
  edit "wifi4"
    set ssid "FOS_QA_100D-IPv6"
    set passphrase *****
    set schedule "always"
  next
end
```

#### 2. Create an IPv6 address for the VAP with DHCP enabled:

```
config system interface
  edit "wifi4"
    set vdom "vdom1"
    set ip 10.40.80.1 255.255.255.0
    set allowaccess ping https http
    set type vap-switch
    set alias "vdom1:"
    set device-identification enable
    set role lan
    set snmp-index 36
    config ipv6
      set ip6-address 2001:10:40:80::1/64
      set ip6-allowaccess ping https http
      set ip6-send-adv enable
      set ip6-manage-flag enable
      set ip6-other-flag enable
    end
  next
end

config system dhcp6 server
  edit 1
```

```

set subnet 2001:10:40:80::/64
set interface "wifi4"
config ip-range
    edit 1
        set start-ip 2001:10:40:80::1000
        set end-ip 2001:10:40:80::1100
    next
end
next
end

```

### 3. Create an IPv6 policy from the VAP to WAN1:

```

config firewall policy
    edit 1
        set name "ipv6"
        set srcintf "wifi4"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end

```

### 4. Verify the IPv6 address in the station list:

#### a. In the FortiGate CLI:

```

# diagnose wireless-controller wlacl -d sta online
vf=4 wtp=3 rId=1 wlan=wifi4 vlan_id=0 ip=10.40.80.2 ip6=2001:10:40:80::1000
mac=b4:ae:2b:cb:d1:72 vci=MSFT 5.0 host=DESKTOP-DO33HQP user= group= signal=-29
noise=-93 idle=1 bw=48 use=5 chan=6 radio_type=11N security=wpa2_only_personal
mpsk=default encrypt=aes cp_authed=no online=yes mimo=2
ip6=fe80::c5c5:6c09:8021:d2d0,88, *2001:10:40:80::1000,8,

```

#### b. In the FortiAP CLI:

```

FortiAP-S221E # sta
wlan00 (FOS_QA_100D-IPv6) client count 1
MAC:b4:ae:2b:cb:d1:72 ip:10.40.80.2 ip_proto:dhcp ip_age:84 host:DESKTOP-DO33HQP
vci:MSFT 5.0
ip6:fe80::c5c5:6c09:8021:d2d0 ip6_proto:arp ip6_age:2 ip6_
rx:101
ip6:2001:10:40:80::1000 ip6_proto:dhcp ip6_age:82 ip6_rx:20
vlanid:0 Auth:Yes channel:6 rate:130Mbps rssi:65dB idle:0s
Rx bytes:256951 Tx bytes:53947 Rx rate:130Mbps Tx rate:130Mbps Rx last:0s Tx
last:0s
AssocID:1 Mode: Normal Flags:f PauseCnt:0
KEY type=aes_ccm pad=0 keyix=65535 keylen=16 flags=3(xmit recv) RSC=0 TSC=0
e7 6f 05 ce 06 e1 4a 9b 3a d4 4f 43 1f 57 bb 49
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
KEY type=aes_ccm pad=0 keyix=1 keylen=16 flags=83(xmit recv dflt) RSC=0 TSC=0
01 47 6f 21 9b ac 73 4b 7c ae 07 66 7e 5a c6 7e
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

```

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FortiAP-S221E #

FortiAP-S221E # usta

WTP daemon STA info:

1/1 b4:ae:2b:cb:d1:72 00:00:00:00:00:00 vId=0 type=wl----sta, vap=wlan00,FOS_
QA_100D-IPv6(0) mpsk=default ip=10.40.80.2/1 host=DESKTOP-DO33HQP vci=MSFT 5.0
os=Windows

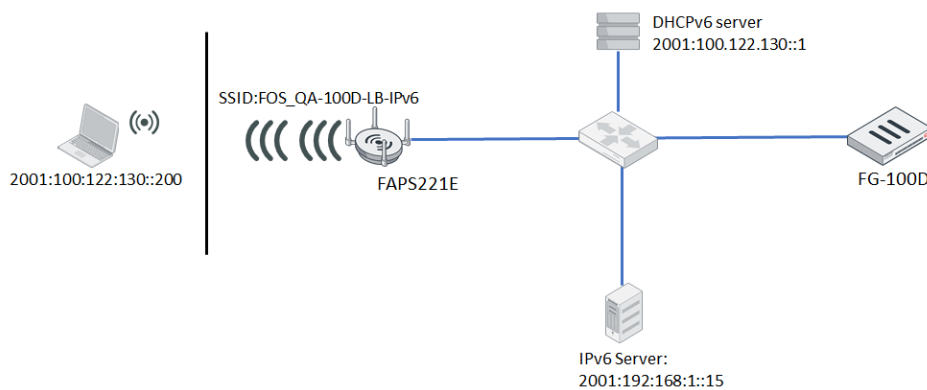
ip6=fe80::c5c5:6c09:8021:d2d0/2 rx=101
ip6=2001:10:40:80::1000/1 rx=21
replycount=0000000000000002

Total STAs: 1

```

## Local bridge mode SSID IPv6 traffic

In the following example, FortiAP S221E is managed by FortiGate 100D through a local NATed switch and broadcasts local bridge mode SSID:FOS\_QA\_100D-LB-IPv6.



### To configure a WiFi client accessing IPv6 local bridge mode traffic:

#### 1. Create a local bridge mode VAP:

```

config wireless-controller vap
  edit "test1"
    set ssid "FOS_QA-100D-LB-IPv6"
    set passphrase *****
    set local-bridging enable
    set schedule "always"
  next
end

```

#### 2. Create an IPv6 DHCP server for the local NATed switch (FortiWiFi 60E is used in this example):

```

config system interface
  edit "internal6"
    set vdom "vdom1"
    set ip 2.2.3.1 255.255.255.0
    set allowaccess ping https http fabric
  next
end

```

```

        set type physical
        set snmp-index 18
    config ipv6
        set ip6-address 2001:100:122:130::1/64
        set ip6-allowaccess ping https http fabric
        set ip6-send-adv enable
        set ip6-manage-flag enable
        set ip6-other-flag enable
    end
next
end

config system dhcp6 server
    edit 1
        set subnet 2001:100:122:130::/64
        set interface "internal6"
        config ip-range
            edit 1
                set start-ip 2001:100:122:130::200
                set end-ip 2001:100:122:130::300
            next
        end
    next
end

```

### 3. Create an IPv6 policy for the local NATed switch:

```

config firewall policy
    edit 2
        set name "ipv6"
        set srcintf "internal6"
        set dstintf "internal7"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end

```

### 4. Verify the IPv6 address in the station list:

#### a. In the FortiGate CLI:

```

# diagnose wireless-controller wlap -d sta online
    vf=4 wtp=3 rId=2 wlan=test1 vlan_id=0 ip=2.2.3.3 ip6=2001:100:122:130::200
mac=f0:98:9d:76:64:c4 vci= host=iPhoneX user= group= signal=-41 noise=-105 idle=18
bw=0 use=5 chan=36 radio_type=11AC security=wpa2_only_personal mpsk=default
encrypt=aes cp_authed=no online=yes mimo=2
    ip6=fe80::82a:9eba:69c5:5454,13, *2001:100:122:130::200,2,

```

#### b. In the FortiAP CLI:

```

FortiAP-S221E # sta
wlan10 (FOS_QA-100D-LB-IPv6) client count 1
    MAC:f0:98:9d:76:64:c4 ip:2.2.3.3 ip_proto:dhcp ip_age:8 host:iPhoneX vci:
    ip6:fe80::82a:9eba:69c5:5454 ip6_proto:arp ip6_age:1 ip6_

```



```

rx:12
                                ip6:2001:100:122:130::200 ip6_proto:dhcp ip6_age:8 ip6_rx:2
vlanid:0 Auth:Yes channel:36 rate:173Mbps rssi:64dB idle:0s
Rx bytes:26654 Tx bytes:27949 Rx rate:78Mbps Tx rate:173Mbps Rx last:0s Tx
last:0s
AssocID:1 Mode: Normal Flags:1000000b PauseCnt:0
KEY type=aes_ccm pad=0 keyix=65535 keylen=16 flags=3(xmit recv) RSC=0 TSC=0
  83 25 7e 72 d2 b1 d2 ef 30 9f 6e 9f 50 e5 6f 5a
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
KEY type=aes_ccm pad=0 keyix=1 keylen=16 flags=83(xmit recv dflt) RSC=0 TSC=0
  1f 25 64 3e 02 4d e2 f1 2c b0 5e 03 ed 99 a4 47
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FortiAP-S221E #

FortiAP-S221E # usta

WTP daemon STA info:

  1/1 f0:98:9d:76:64:c4 00:00:00:00:00:00 vId=0 type=wl----sta, vap=wlan10,FOS_
QA-100D-LB-IPv6(0) mpsk=default ip=2.2.3.3/1 host=iPhoneX vci= os=iOS
      ip6=fe80::82a:9eba:69c5:5454/2 rx=12
      ip6=2001:100:122:130::200/1 rx=2
      replycount=00000000000000002

Total STAs: 1

```

## CLI commands for IPv6 rules

The following IPv6 rules can be used in VAP configurations:

Command	Description
drop-icmp6ra	Drop ICMPv6 router advertisement (RA) packets that originate from wireless clients.
drop-icmp6rs	Drop ICMPv6 router solicitation (RS) packets to be sent to wireless clients.
drop-llmnr6	Drop Link-Local Multicast Name Resolution (LLMNR) packets.
drop-icmp6mld2	Drop ICMPv6 Multicast Listener report V2 (MLD2) packets.
drop-dhcp6s	Drop DHCPv6 server generated packets that originate from wireless clients.
drop-dhcp6c	Drop DHCPv6 client generated packets to be sent to wireless clients.
ndp-proxy	Enable IPv6 NDP proxy; send back NA on behalf of the client and drop the NS.
drop-ns-dad	Drop ICMPv6 NS DAD when target address is not found in the NDP proxy cache.
drop-ns-nondad	Drop ICMPv6 NS non-DAD when target address is not found in the NDP proxy cache.

**To configure IPv6 rules on a VAP:**

```
config wireless-controller vap
  edit "wifi4"
    set ssid "FOS_QA_100D-IPv6"
    set passphrase *****
    set schedule "always"
    set ipv6-rules drop-icmp6ra drop-icmp6rs drop-llmnr6 drop-icmp6mld2 drop-dhcp6s
drop-dhcp6c ndp-proxy drop-ns-dad drop-ns-nondad
  next
end
```

The IPv6 rules settings can be pushed to a FortiAP when the VAP is broadcast.

**To view the pushed settings on the FortiAP:**

```
FortiAP-S221E # iwpriv wlan00 get_bmcs6
wlan00      get_bmcs6:991  (0x3df)
00000001 icmp6-ra          : yes
00000002 icmp6-rs          : yes
00000004 dhcp6-server      : yes
00000008 dhcp6-client      : yes
00000010 llmnr             : yes
00000040 icmp6-mld2        : yes
00000080 ndp-proxy         : yes
00000100 ns-dad            : yes
00000200 ns-nondad         : yes
```

## Support for spectrum analysis of FortiAP E models

Spectrum analysis is available for FortiAP E models running 6.4.0 and later firmware. The analysis is visible in the GUI through the *Managed FortiAPs* page. Spectrum analysis can also be performed in the CLI.

To start or stop the spectrum analysis:

```
execute wireless-controller spectral-scan <wtp-id> <radio-id> <on | off> <duration>
<channel> <report-interval>
```

To verify the results:

```
diagnose wireless-controller wlac -c rf-sa <wtp-id> <radio-id> <channel>
get wireless-controller spectral-info <wtp-id> <radio-id>
```

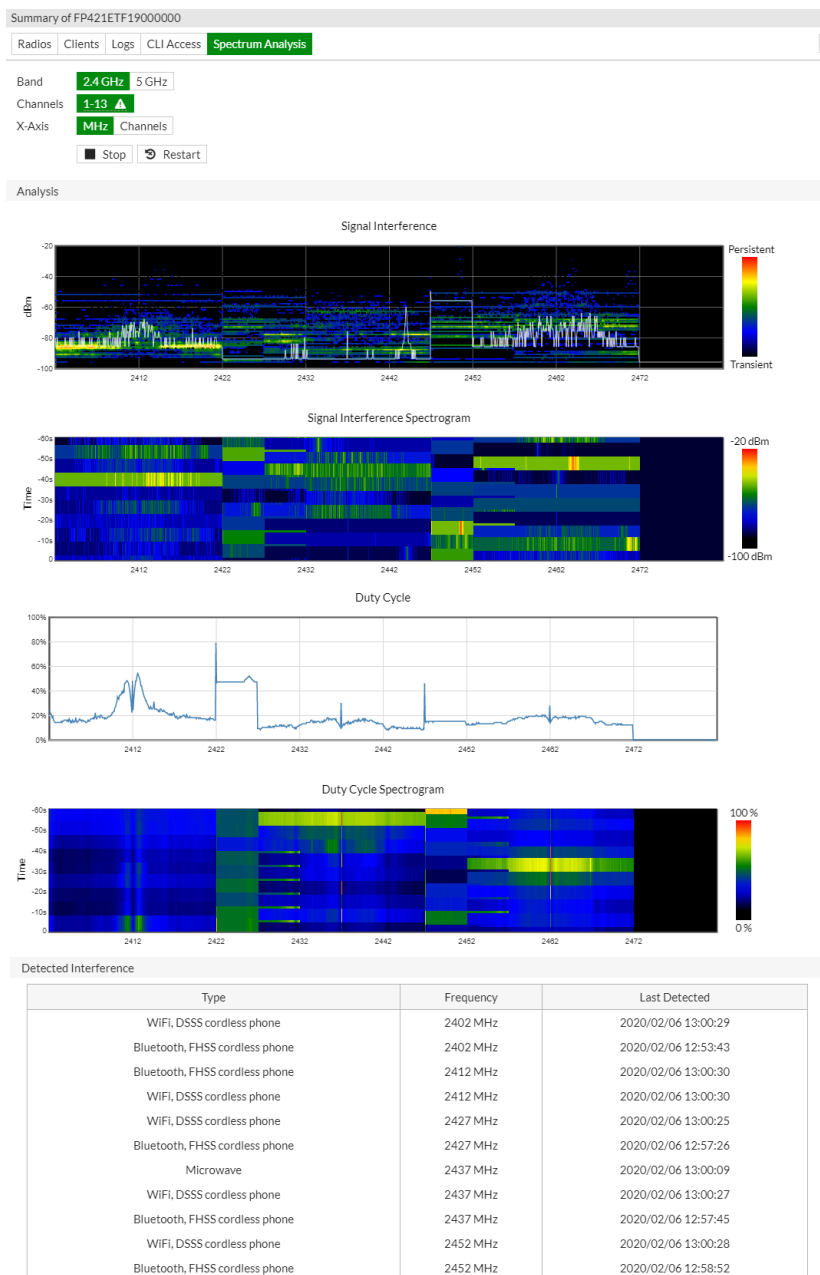
The following examples use a FortiAP 421E (radio 1 at 2.4 GHz and radio 2 at 5 GHz) that is managed by a FortiGate 80E-POE.

## To view spectrum analysis in the GUI:

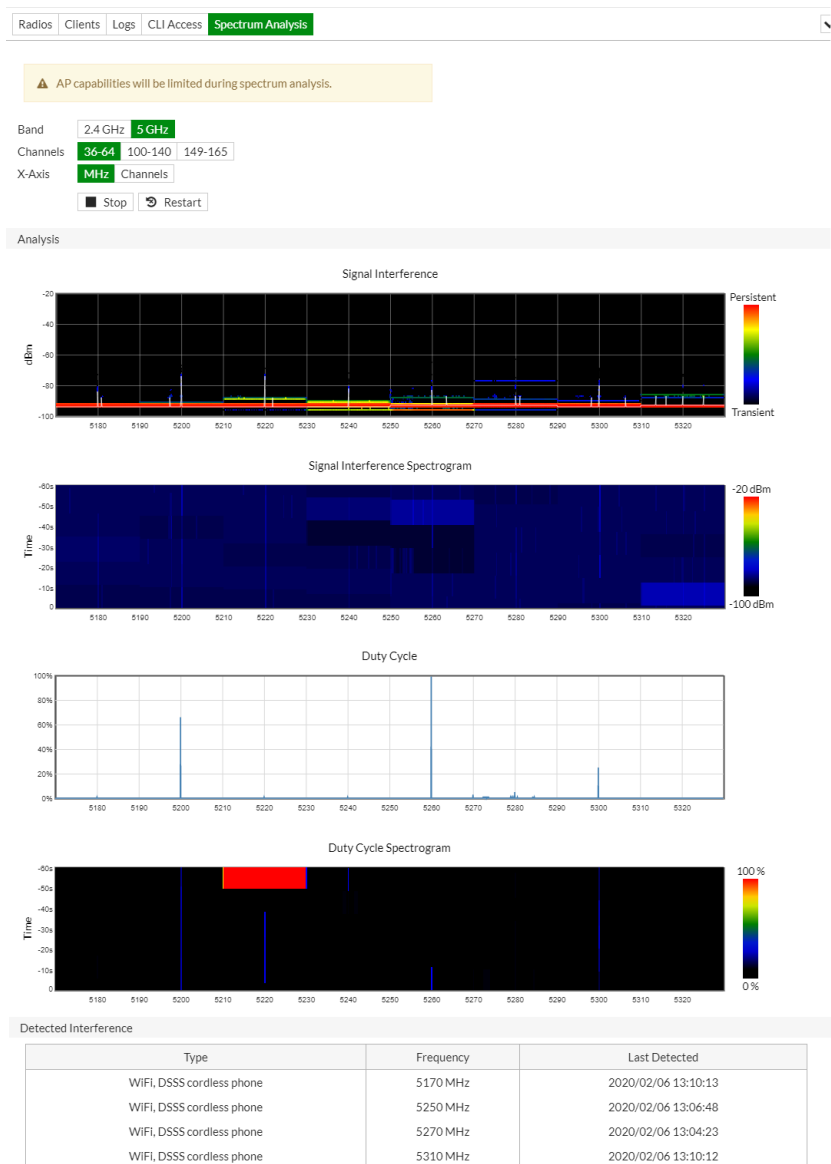
1. Change the radio mode:
  - a. Go to *WiFi & Switch Controller > FortiAP Profiles* and double-click the FortiAP to edit the profile.
  - b. In the *Radio 1* and *Radio 2* sections for *Mode*, select *Dedicated Monitor*.

The screenshot shows the FortiAP Profile configuration page. The 'Name' field is '421E'. The 'Platform' is 'FAP421E'. The 'Country / Region' is 'Use default (United States)'. The 'AP login password' is 'Set Leave Unchanged Set Empty'. The 'Administrative access' section has checkboxes for 'HTTPS' (checked), 'SSH' (checked), and 'SNMP' (unchecked). The 'Radio 1' section has a 'Mode' dropdown set to 'Dedicated Monitor' and a 'WIDS profile' toggle. The 'Radio 2' section also has a 'Mode' dropdown set to 'Dedicated Monitor' and a 'WIDS profile' toggle. The 'Location Based Services' section has a 'FortiPresence' dropdown set to 'Disable'. The 'Ekahau blink' and 'AeroScout' toggles are also visible.

- c. Click *OK*.
  2. Go to *WiFi & Switch Controller > Managed FortiAPs*.
  3. In the table, hover over the AP so the context menu appears and click *Details*. The summary pane appears.
  4. Click *Spectrum Analysis*.
  5. Click a band frequency to view the analysis for: *Signal Interference*, *Signal Interference Spectrogram*, *Duty Cycle*, *Duty Cycle Spectrogram*, and *Detected Interference* (list).
- Analysis for 2.4 GHz:



Analysis for 5 GHz:



6. Click *Close*.

### To change the radio mode in the CLI:

```

config wireless-controller wtp-profile
  edit "421E"
    config platform
      set type 421E
    end
    config radio-1
      set mode monitor
    end
    config radio-2
      set mode monitor
    end
  next
end
  
```

**To view spectrum analysis for radio 1 in the CLI:****1. Start the spectrum analysis on channel 1:**

```
# execute wireless-controller spectral-scan FP421ETF19000000 1 on 30 1 1000
```

**2. View the analysis results:**

```
# diagnose wireless-controller wlac -c rf-sa FP421ETF19000000 1 1
-----RF Spectrum Data 1-----
rId: 1 Age: 24 gen 27 rssi: 11 nf: -96 bw: 1 Freq: 2412 Chan: 1 Cnt bin 256
Interf: 0 (idx,duty_max,duty,pwr_max,pwr)
  0 45 14 -67 -89 1 45 14 -60 -89 2 44 14 -63 -89 3
44 13 -57 -83 - 5 43 12 -67 -89 6 43 11 -67 -89 7
  4 44 13 -61 -89 9 42 10 -67 -89 10 41 10 -67 -83 - 11
42 11 -67 -89 13 42 10 -67 -89 14 41 10 -67 -83 - 15
  8 42 10 -67 -89 17 41 10 -67 -89 18 41 10 -67 -89 19
41 10 -67 -89 21 41 10 -67 -89 22 41 10 -67 -89 23
 12 41 10 -67 -89 16 41 10 -61 -89 20 41 10 -67 -89
41 10 -67 -89 42 10 -67 -79 -
```

```
# get wireless-controller spectral-info FP421ETF19000000 1
=====
Spectrum info for band freq [2402, 2482] chan [1,13]: (idx,age,gen,duty_max,duty,pwr_max,pwr)
2402 0 1 7 19 19 -21 -83 - 1 1 7 18
 18 -33 -83 - 2 1 7 18 18 -35 -83 - 3 1 7 17
  2 -39 -83 - 4 1 7 17 17 -43 -83 - 5 1 7 16
 17 -47 -83 - 6 1 7 15 15 -33 -83 - 7 1 7 15
 16 -45 -83 - 8 1 7 14 14 -59 -83 - 9 1 7 14
  6 -53 -83 - 10 1 7 14 14 -59 -83 - 11 1 7 14
 15 -59 -83 -
```

**3. Stop the spectrum analysis on radio 1:**

```
# execute wireless-controller spectral-scan FP421ETF19000000 1 off
```

**4. Verify the analysis has stopped:**

```
# get wireless-controller spectral-info FP421ETF19000000 1
=====
No spectrum info is found for band freq [2402, 2482] chan [1,13]
=====
No spectrum info is found for band freq [5170, 5330] chan [36,64]
=====
No spectrum info is found for band freq [5490, 5710] chan [100,140]
=====
No spectrum info is found for band freq [5735, 5835] chan [149,165]
FortiGate-80E-POE # diagnose wireless-controller wlac -c rf-sa FP421ETF19000000 1 1
-----Total 0 RF Spectrum Datas-----
```

**To view spectrum analysis for radio 2 in the CLI:****1. Start the spectrum analysis on all channels:**

```
# execute wireless-controller spectral-scan FP421ETF19000000 2 on
```

**2. View the analysis results:**

```
# get wireless-controller spectral-info FP421ETF19000000 2
=====
No spectrum info is found for band freq [2402, 2482] chan [1,13]
=====
Spectrum info for band freq [5170, 5330] chan [36,64]: (idx,age,gen,duty_max,duty,pwr_
max,pwr)
5170      0      24      9      0      0      -92      -94      1      24      9      0
0      -92      -94
0      2      24      9      0      0      -92      -94      3      24      9      0
0      -92      -94
0      4      24      9      0      0      -92      -94      5      24      9      0
0      -92      -94
0      6      24      9      0      0      -92      -94      7      24      9      0
0      -92      -94
0      8      24      9      0      0      -92      -94      9      24      9      0
0      -92      -94
0      10     24      9      0      0      -92      -94     11      24      9      0
0      -92      -94
0      12     24      9      0      0      -92      -94     13      24      9      0
0      -92      -94
0      14     24      9      0      0      -92      -94     15      24      9      0
0      -92      -94
```

**3. Check the spectrum analysis results on specific channels:**

```
# diagnose wireless-controller wlac -c rf-sa FP421ETF19000000 2 36
-----RF Spectrum Data 1-----
rId: 2 Age: 6 gen 7 rssi: 2 nf: -96 bw: 1 Freq: 5180 Chan: 36 Cnt bin 256
Interf: 0 (idx,duty_max,duty,pwr_max,pwr)
0 0 0 -92 -94 1 0 0 -92 -94 2 0 0 -92 -94 3
0 0 -92 -94
4 0 0 -92 -94 5 0 0 -92 -94 6 0 0 -92 -94 7
0 0 -92 -94
8 0 0 -92 -94 9 0 0 -92 -94 10 0 0 -92 -94 11
0 0 -92 -94
12 0 0 -92 -94 13 0 0 -92 -94 14 0 0 -92 -94 15
0 0 -92 -94
16 0 0 -92 -94 17 0 0 -92 -94 18 0 0 -92 -94 19
0 0 -92 -94
20 0 0 -92 -94 21 0 0 -92 -94 22 0 0 -92 -94 23
0 0 -92 -94
24 0 0 -92 -94 25 0 0 -92 -94 26 0 0 -92 -94 27
0 0 -92 -94
28 0 0 -92 -94 29 0 0 -92 -94 30 0 0 -92 -94 31
0 0 -92 -94

# diagnose wireless-controller wlac -c rf-sa FP421ETF19000000 2 165
-----RF Spectrum Data 1-----
rId: 2 Age: 22 gen 6 rssi: 11 nf: -96 bw: 1 Freq: 5825 Chan: 165 Cnt bin 256
Interf: 0 (idx,duty_max,duty,pwr_max,pwr)
```

```

0 0 0 -90 -90      1 0 0 -90 -90      2 0 0 -90 -90      3
0 0 -90 -90
4 0 0 -90 -90      5 0 0 -90 -90      6 0 0 -90 -90      7
0 0 -90 -90
8 0 0 -90 -90      9 0 0 -90 -90      10 0 0 -90 -90      11
0 0 -90 -90
12 0 0 -90 -90     13 0 0 -90 -90     14 0 0 -90 -90     15
0 0 -90 -90
16 0 0 -90 -90     17 0 0 -90 -90     18 0 0 -90 -90     19
0 0 -90 -90
20 0 0 -90 -90     21 0 0 -90 -90     22 0 0 -90 -90     23
0 0 -90 -90
24 0 0 -90 -90     25 0 0 -90 -90     26 0 0 -90 -90     27
0 0 -90 -90
28 0 0 -90 -90     29 0 0 -90 -90     30 0 0 -90 -90     31
0 0 -90 -90

```

#### 4. Stop the spectrum analysis on radio 2:

```
# execute wireless-controller spectral-scan FP421ETF19000000 2 off
```

#### 5. Verify the analysis has stopped:

```
# get wireless-controller spectral-info FP421ETF19000000 2
=====
No spectrum info is found for band freq [2402, 2482] chan [1,13]
=====
No spectrum info is found for band freq [5170, 5330] chan [36,64]
=====
No spectrum info is found for band freq [5490, 5710] chan [100,140]
=====
No spectrum info is found for band freq [5735, 5835] chan [149,165]
=====
```

## Increase in maximum number of managed FortiAPs

The maximum number of managed FortiAPs has increased in some FortiGate E models for added wireless capability and scalability.

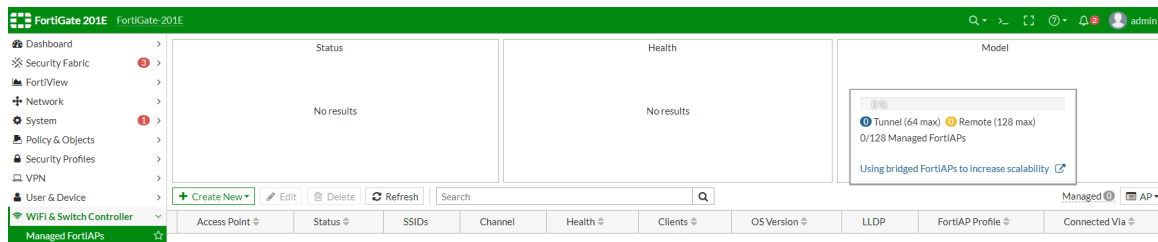
The following comparison table shows the maximum number of FortiAPs supported in FortiGate E models:

FGT Model	FortiOS 6.2	FortiOS 6.4
FGT200E, FGT201E	128	256
FGT3960E, FGT3980E	4,096	8,192

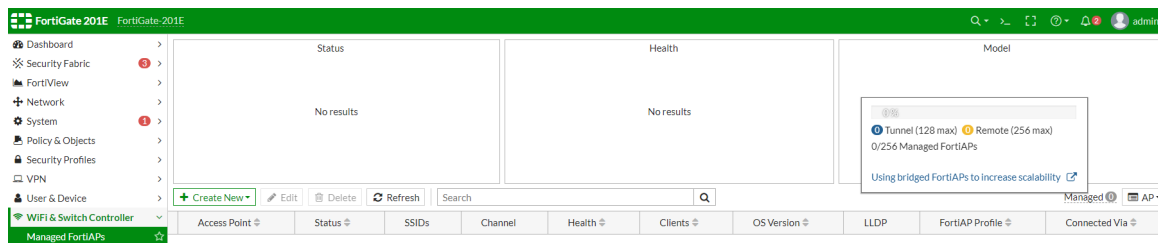
#### To view the maximum in the GUI:

1. Go to *Wifi & Switch controller > Managed FortiAPs*.
2. At the right-side of the page, hover over *Managed*. The new maximum appears in the information window. FGT201E can support a maximum of *128 Managed FortiAPs* with FortiOS 6.2.

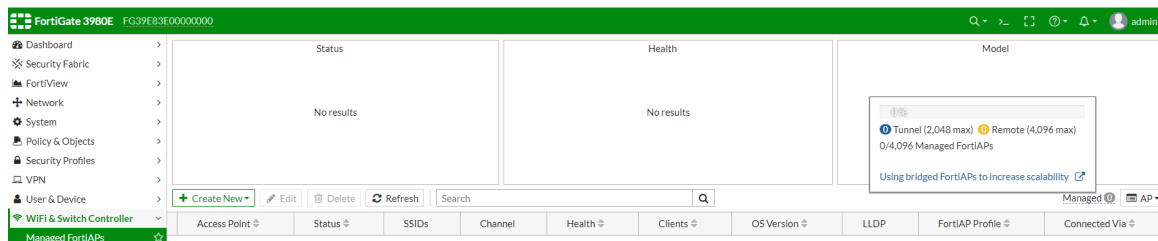




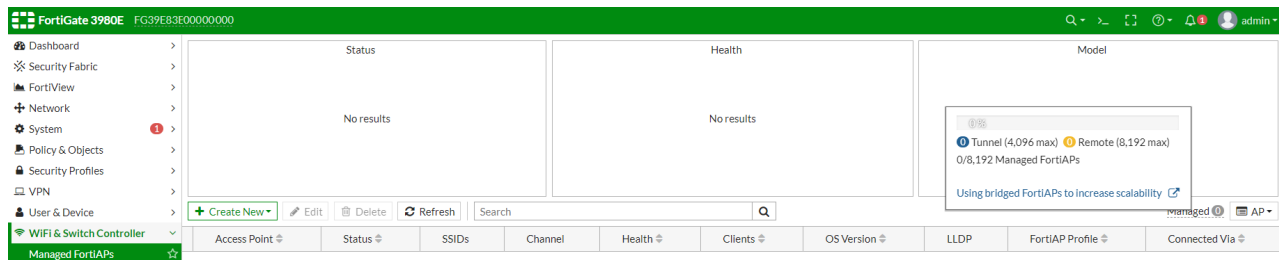
FGT201E can support a maximum of 256 FortiAPs with FortiOS 6.4.



FGT3980E can support a maximum of 4,096 FortiAPs with FortiOS 6.2.



FGT3980E can support a maximum of 8,192 FortiAPs with FortiOS 6.4.



## Even distribution of FortiAP reports

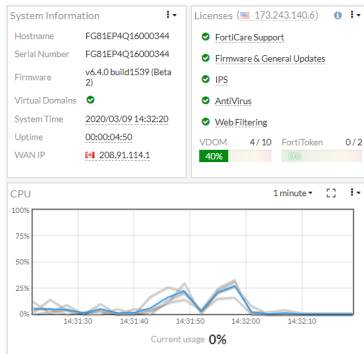
Reporting intervals for FortiAP are now evenly distributed to prevent spikes in CPU usage in FortiGates that manage a large number of AP devices.

FortiAP sends periodic reports to FortiGate when WIDS profiles, DARRP, or auto-power-level are enabled in WTP profiles. Before this improvement was implemented, these periodic reports would frequently reach the wireless controller at the same time, causing spikes in CPU usage.

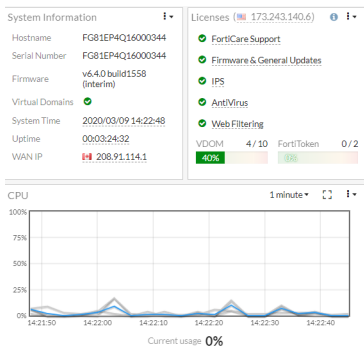
## GUI

The following images compare the CPU usage in a FortiGate that manages 16 FortiAPs before and after the improvement was implemented.

Before the improvement, CPU usage is above 25%. The spike in usage can go as high as 90% if the FortiGate manages more than 16 devices.



After the improvement is implemented, CPU usage is approximately 10% in the same FortiGate.



## CLI

The following examples show the improvements in the CLI for the same FortiGate device.

In this example, you can see 16 wireless sessions in the CLI.

```
FG81EP4Q16000344 (root) # diag wire wlac -c ws | grep "WTP session"
WTP session : 0-10.43.1.1:62332 CWAS_RUN
WTP session : 0-10.43.1.1:62350 CWAS_RUN
WTP session : 0-10.43.1.1:62356 CWAS_RUN
WTP session : 0-10.43.1.1:62357 CWAS_RUN
WTP session : 0-10.43.1.1:62325 CWAS_RUN
WTP session : 0-10.43.1.1:15246 CWAS_RUN
WTP session : 0-10.43.1.1:62362 CWAS_RUN
WTP session : 0-10.43.1.1:62364 CWAS_RUN
WTP session : 0-10.43.1.1:62366 CWAS_RUN
WTP session : 0-10.43.1.1:62367 CWAS_RUN
WTP session : 0-10.43.1.1:62319 CWAS_RUN
WTP session : 0-10.43.1.1:62321 CWAS_RUN
WTP session : 0-10.43.1.1:62320 CWAS_RUN
WTP session : 0-10.43.1.1:62370 CWAS_RUN
WTP session : 0-10.43.1.1:62323 CWAS_RUN
WTP session : 0-10.43.1.1:62329 CWAS_RUN
```

Before the improvement is implemented, the FortiAP WTP reports are not indexed, which can cause spikes in CPU usage.

```
FG81EP4Q16000344 (root) # diag wireless-controller wlac -c ws | grep report
FG81EP4Q16000344 (root) #
```

After the improvement is implemented, the AC assigns a wtp-report-index to each managed FortiAP, preventing spikes in CPU usage.

```
FG81EP4Q16000344 (root) # diag wireless-controller wlac -c ws | grep report
wtp-report-index : 1
wtp-report-index : 2
wtp-report-index : 3
wtp-report-index : 4
wtp-report-index : 5
wtp-report-index : 6
wtp-report-index : 7
wtp-report-index : 8
wtp-report-index : 9
wtp-report-index : 10
wtp-report-index : 11
wtp-report-index : 12
wtp-report-index : 13
wtp-report-index : 14
wtp-report-index : 15
wtp-report-index : 16
```

You can see the value for the wtp-report-index when you filter the data by device. In this example, the report index is 16.

```
FG81EP4Q16000344 (root) # diag wireless-controller wlac -c ws 10.231.40.15
-----WTP SESSION 1-----
WTP session : 0-10.43.1.1:62433 CWAS_RUN
Ctrl in_ifIdx : 5/wan1
indev : 5/wan1
Data in_ifIdx : 5/wan1
indev : 0/
mesh uplink : ethernet
id : FP423E3X16000304
mgmt_vlanid : 0
wtp_wanlan_mode : wan-only
refcnt : 10
deleted : no
plain_ctl : disabled
wtp-mode : normal
wtp-report-index : 16
data-chan-sec : clear-text
ctl-msg-offload : ac=01ff/wtp_loc=01ff/wtp_rem=01ff/oper=01ff
session_id : 70386ec03c8bdcd630efda365b3f9ce0
ehapd cfg : done
message queue : 0/128 max 65
tId_10_sec : 3537
Ekahau : disabled
Aeroscout : disabled
FortiPresence : disabled
Radio 1 : AP
wlan cfg : 81ep_ssid1 81ep_ssid2 81ep_ssid4 81ep_wpa3_sae
vap-01(1) : 81ep_ssid1 90:6c:ac:dc:60:b0 lsw FOS-QA-Bruce_81ep1 Config success State
RUN
vap-02(2) : 81ep_ssid2 90:6c:ac:dc:60:b1 lsw FOS-QA-Bruce_81ep2 Config success State
RUN
vap-03(3) : 81ep_ssid4 90:6c:ac:dc:60:b2 lsw FOS-QA-BRUCE_roaming Config success
State RUN
```

```

vap-04(4) : 81ep_wpa3_sae 90:6c:ac:dc:60:b3 lsw 81ep_wpa3_sae Config success State
INIT
Radio 2 : AP
wlan cfg : 81ep_ssid1 81ep_ssid2 81ep_ssid4 81ep_wpa3_sae
vap-01(1) : 81ep_ssid1 90:6c:ac:dc:60:b8 lsw FOS-QA-Bruce_81ep1 Config success State
RUN
vap-02(2) : 81ep_ssid2 90:6c:ac:dc:60:b9 lsw FOS-QA-Bruce_81ep2 Config success State
RUN
vap-03(3) : 81ep_ssid4 90:6c:ac:dc:60:ba lsw FOS-QA-BRUCE_roaming Config success
State RUN
vap-04(4) : 81ep_wpa3_sae 90:6c:ac:dc:60:bb lsw 81ep_wpa3_sae Config success State
N/A
Radio 3 : Not Exist
Radio 4 : Not Exist
Radio 5 : Not Exist

```

You can also see the device's wtp-report-index value when you view the WTP configuration in FortiAP.

```

FortiAP-423E # cw_diag -c wtp-cfg
WTP Configuration
  name : FortiAP-423E
  loc : N/A
  ap mode : thin AP
  fmwap : FG81EP4Q16000344, (12ac979c, 5e693999, 1), 1800, 0
  atf mode : disabled
  dual-5g mode : disabled
  poe mode : auto
  poe mode oper : 802.3at
  led mode : normal
  led schedules : SMTWTFS 00:00->00:00,
  WAN port cnt : 2
  lan1 : carrier=1, speed=1000, duplex=full
  lan2 : carrier=0, speed=0, duplex=
  energy-efficient-eth : disable
  extension info enable: enable
  allowaccess : https ssh
  lldp enable : enable
wtp-report-index : 16
  ctl-msg-offload : ac=01ff/wtp=01ff/oper=01ff
  radio cnt : 2
  sta info : 0/0
  echo-interval : 30
  keep-alive-interval : 30
  max-retransmit : 3
  dc-dead-interval : 120
  discovery-interval : 5
  report-interval : 30
  sta-stats-interval : 1
  vap-stats-interval : 15
  radio-stats-interval : 15
  sta-cap-interval : 30
  idle-timeout : 300
  fpresence-interval : 3600, 30
  statistics-interval : 120
  fsm-state : RUN 439
  wtp-ip-addr : 10.231.40.15:25246 - 10.231.40.15:36529
  ac-ip-addr : 172.18.56.46:5246 - 172.18.56.46:5247 DHCP
  base-mac : 90:6c:ac:dc:60:a8

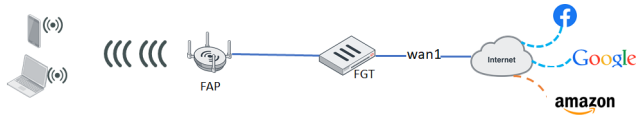
```

```
bulk data seq num : -1
ap-mgmt-vlanid : 0
ac-cert-version : 1
cert-version-oper : 1
data-chan-sec-cfg : clear-text dtls ipsec
data-chan-sec-oper : clear-text
ip-frag-prevent : TCP_MSS (ul_mtu=1500 dl_mtu=1500)
ekahau : disabled
aeroscout : disabled
data-ethernet-II : disabled
fortipresence : disabled, ble enabled, rogue disabled, unassoc_sta enabled, freq 30
server 0.0.0.0:3000 secret csum [0xc6a7] project [fortipresence]
LAN mode : disabled
LAN port cnt : 0
encrypt_key[0-15] : 14-aa-7f-3e-34-a1-83-e7-ca-51-49-2c-e3-64-b3-03
encrypt_key[16-31] : 70-1a-42-5b-a5-5d-79-f0-c4-6e-e0-2f-a8-81-58-13
```

## View detailed information for individual WiFi connections

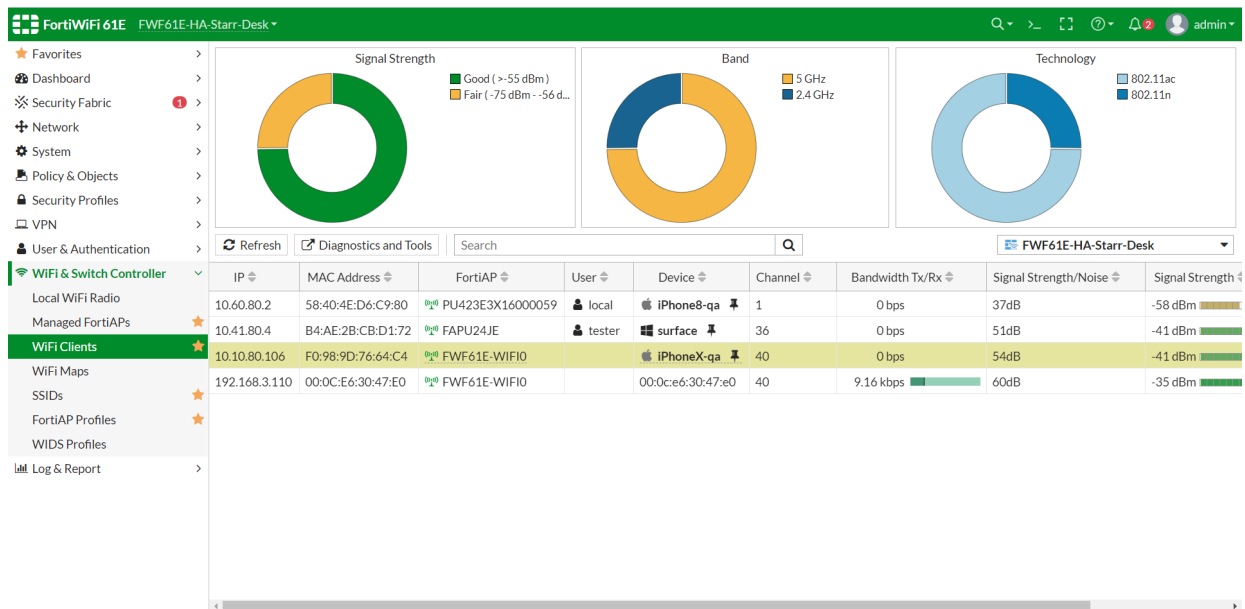
Administrators can use the GUI to view detailed information about the health of individual WiFi connections from the *Dashboard* or the *WiFi Clients* console. You can also *Quarantine* or *Disassociate* a wireless client. The information in the *FortiView* page is now displayed as tabs in the summary window for each wireless client.

### Sample topology

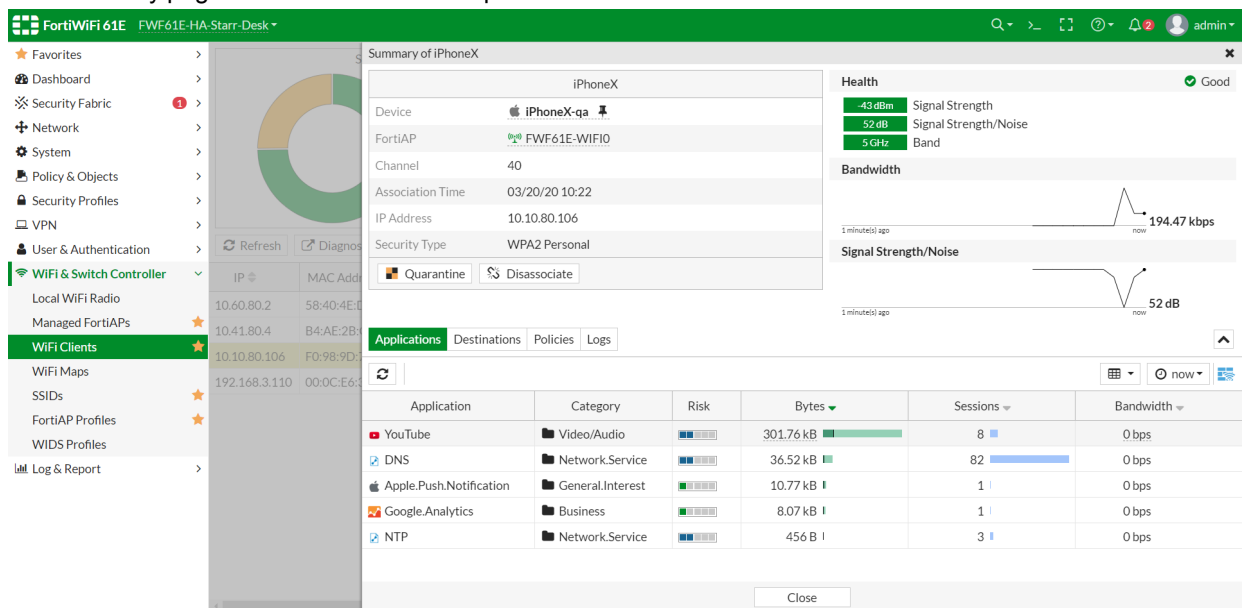


### To view the summary page for a wireless client in the GUI:

1. Go to *WiFi & Switch Controller > WiFi Clients*, and select a wireless client. Click *Diagnostics and Tools* to the right side of the *Refresh* icon.



2. The summary page for the selected client opens.



3. On the summary page, click *Quarantine*. The *Quarantine Host* dialog opens. Click *OK* to quarantine the selected wireless client, and close the dialog.

Summary of iPhone

Device: iPhone8-qa

FortiAP: PU423E3X16000059

User: local

Channel: 1

Association Time: 03/20/20 10:17

IP Address: 10.60.80.2

Security Type: WPA2 Enterprise

Uplink Interface: FWF61E-WIFI0

Quarantine

Applications

Application	Category	Risk	Bytes	Sessions	Bandwidth
IMAPS	Email		18.22 kB	2	0 bps

4. On the summary page, click the *Disassociate* icon. The *Confirm* dialog opens. Click *OK* to dissociate the selected wireless client, and close the dialog.

Summary of iPhone

Device: iPhone8-qa

FortiAP: PU423E3X16000059

User: local

Channel: 1

Association Time: 03/20/20 10:17

IP Address: 10.60.80.2

Security Type: WPA2 Enterprise

Uplink Interface: FWF61E-WIFI0

Quarantine

Disassociate

Confirm

Client will be dissociated from FortiAP.

OK

Cancel

5. From the summary page, the *Health* section displays the overall health for the wireless connection. The overall health of the connection is:
- *Good* if the value range for all three conditions are Good.
  - *Fair* or *Poor* if one of the three conditions is *Fair* or *Poor*.

Condition	Value range
Signal Strength	<ul style="list-style-type: none"> <li>• <i>Good</i> &gt; -56dBm</li> <li>• -56dBm &gt; <i>Fair</i> &gt; -75dBm</li> <li>• <i>Poor</i> &lt; -75dBm</li> </ul>

Condition	Value range
<b>Signal Strengthen</b>	<ul style="list-style-type: none"> <li>• <i>Good</i> &gt; 39dBm</li> <li>• 20dBm &lt; <i>Fair</i> &lt; 39dBm</li> <li>• <i>Poor</i> &lt; 20dBm</li> </ul>
<b>Band</b>	<ul style="list-style-type: none"> <li>• <i>Good</i> = 5G band</li> <li>• <i>Fair</i> = 2.4G band</li> </ul>

Example of an overall health status of *Good*.

The screenshot shows the FortiWiFi 61E management console. The left sidebar lists various configuration options, with 'WiFi & Switch Controller' and 'WiFi Clients' highlighted. The main panel displays the 'Summary of DESKTOP-DO33HQP'. The 'Health' section shows a green 'Good' status. The 'Signal Strength' is -37 dBm, 'Signal Strength/Noise' is 55 dB, and 'Band' is 5 GHz. The 'Bandwidth' section shows a line graph for 'Signal Strength/Noise' at 0 bps. The 'Applications' table lists the following data:

Application	Category	Risk	Bytes	Sessions	Bandwidth
TCP/7680			35.24 MB	3	0 bps
HTTPS.BROWSER	Web.Client		1.14 MB	8	2.90 kbps
SSL	Network.Service		3.64 kB	2	0 bps
TCP/8013			528 B	2	0 bps

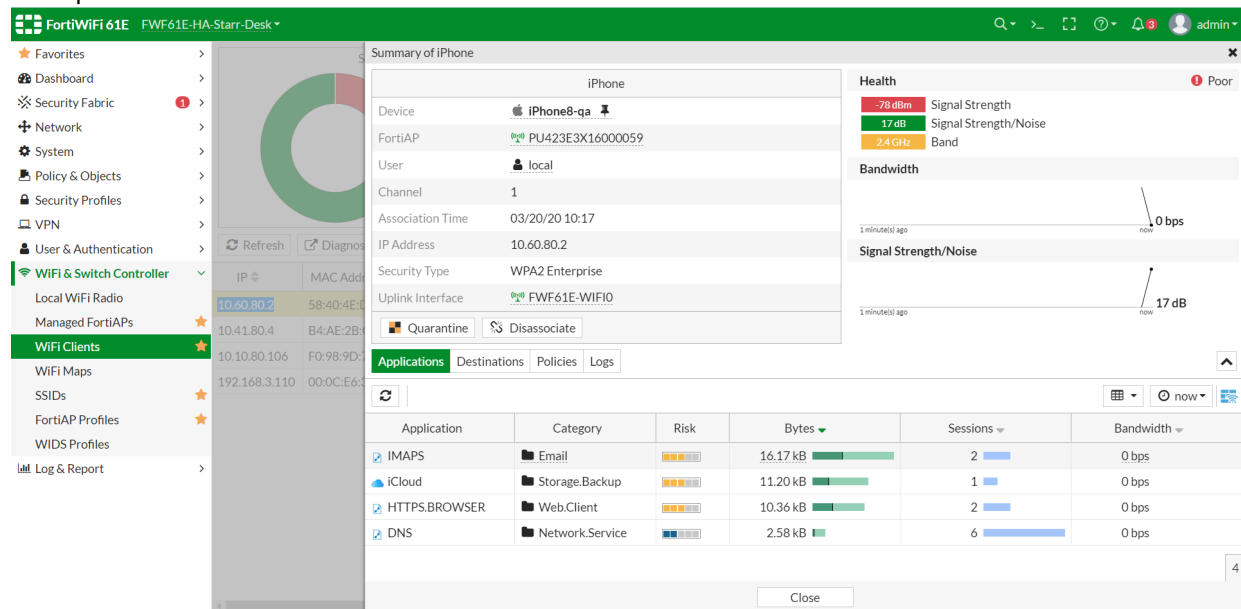
Example of an overall health status of *Fair*.

The screenshot shows the FortiWiFi 61E management console. The left sidebar lists various configuration options, with 'WiFi & Switch Controller' and 'WiFi Clients' highlighted. The main panel displays the 'Summary of iPhone'. The 'Health' section shows a yellow 'Fair' status. The 'Signal Strength' is -61 dBm, 'Signal Strength/Noise' is 34 dB, and 'Band' is 2.4 GHz. The 'Bandwidth' section shows a line graph for 'Signal Strength/Noise' at 0 bps. The 'Applications' table lists the following data:

Application	Category	Risk	Bytes	Sessions	Bandwidth
IMAPS	Email		18.22 kB	2	0 bps
DNS	Network.Service		469 B	1	0 bps



Example of an overall health status of *Poor*.



6. The summary page contains four FortiView tabs:

- *Applications*
- *Destinations*
- *Policies*
- *Logs*

The image displays three sequential screenshots of the FortiWiFi 61E management interface, showing the configuration and monitoring of a client connection. The interface is titled "FortiWiFi 61E FWF61E-HA-Starr-Desk" and includes a sidebar with navigation options like Dashboard, Security Fabric, Network, System, Policy & Objects, Security Profiles, VPN, User & Authentication, and WiFi & Switch Controller.

**Top Screenshot: Applications View**

Summary of F0:98:9D:76:64:C4

Device: iPhoneX-qa  
FortiAP: FWF61E-WIFI0  
Channel: 40  
Association Time: 03/20/20 09:48  
IP Address: 10.10.80.106  
Security Type: WPA2 Personal

Health: Good  
Signal Strength: -47 dBm  
Signal Strength/Noise: 48 dB  
Band: 5 GHz

Bandwidth: 12.22 kbps

Signal Strength/Noise: 48 dB

Applications Table:

Application	Category	Risk	Bytes	Sessions	Bandwidth
Apple.Store	GeneralInterest	Low	2.11 MB	21	1.69 Mbps
HTTPS.BROWSER	Web.Client	Low	254.41 kB	22	93.98 kbps
YouTube	Video/Audio	Low	150.52 kB	8	74.55 kbps
Apple.Services	GeneralInterest	Low	82.91 kB	5	52.23 kbps
Google.Ads	GeneralInterest	Low	74.47 kB	5	26.74 kbps
DNS	Network.Service	Low	27.94 kB	60	12.71 kbps

**Middle Screenshot: Destinations View**

Summary of F0:98:9D:76:64:C4

Device: iPhoneX-qa  
FortiAP: FWF61E-WIFI0  
Channel: 40  
Association Time: 03/20/20 09:48  
IP Address: 10.10.80.106  
Security Type: WPA2 Personal

Health: Good  
Signal Strength: -47 dBm  
Signal Strength/Noise: 48 dB  
Band: 5 GHz

Bandwidth: 0 bps

Signal Strength/Noise: 48 dB

Destinations Table:

Destination	Application	Bytes	Sessions	Bandwidth
23.36.176.42	Apple.Store	1.94 MB	12	0 bps
play.googleapis.com (172.217.175.42)	YouTube	56.46 kB	1	16 bps
partnerad.l.doubleclick.net (172.217.25.66)	Google.Ads	44.67 kB	1	0 bps
montrealgazette.com (192.0.79.32)	HTTPS.BROWSER	44.33 kB	1	0 bps
lytting.com (216.58.197.142)	YouTube	36.62 kB	1	0 bps
e8037.e2.akamaiedge.net (23.58.133.112)	HTTPS.BROWSER	22.19 kB	3	0 bps

**Bottom Screenshot: Policies View**

Summary of F0:98:9D:76:64:C4

Device: iPhoneX-qa  
FortiAP: FWF61E-WIFI0  
Channel: 40  
Association Time: 03/20/20 09:48  
IP Address: 10.10.80.106  
Security Type: WPA2 Personal

Health: Good  
Signal Strength: -45 dBm  
Signal Strength/Noise: 50 dB  
Band: 5 GHz

Bandwidth: 0 bps

Signal Strength/Noise: 50 dB

Policies Table:

Policy	Policy Type	Source Interface	Destination Interface	Bytes	Sessions	Bandwidth
w (1)	IPv4	FOS_QA_Starr-HA-61E-PSK (wifi)	wan1	2.62 MB	128	40 bps

7. Go to *Dashboard > WiFi*. Click the *Clients By FortiAP* widget to view the drill-down information for the wireless client.



## VLAN probe report

FortiGate devices that manage FortiAPs have the ability to probe VLANs and subnets connected to an access point. Use the VLAN probe wireless tool to help troubleshoot why users cannot connect to the Internet.

### GUI

To perform a VLAN probe in the GUI:

1. Go to *WIFI & Switch Controller > Managed FortiAPs*.
2. Right click a FortiAP entry, and select *View More Details*.

The screenshot shows the FortiGate GUI for a FortiGate-81E-POE. The left sidebar lists various configuration sections, with 'WIFI & Switch Controller' expanded. Under this section, 'Managed FortiAPs' is selected. The main area displays three donut charts: 'Status' (showing 'Waiting for Author...' and 'Online'), 'Health' (showing 'Fair'), and 'Model' (showing 'FAP231E' and 'FAP5423E'). Below the charts is a table of managed FortiAPs. The table has columns for Access Point, Status, SSIDs, Channel, Health, Clients, and OS Version. Two entries are visible: 'FP231ETF20000458' (Waiting for Authorization) and 'PS423E3X16000075' (Online). A context menu is open over the 'PS423E3X16000075' entry, showing options like 'Edit', 'View More Details', 'Delete', 'Upgrade', 'Authorize', 'Deauthorize', 'Restart', 'Assign Profile', 'Locate in WiFi Maps', 'LED Blink', 'Edit in CLI', and 'Connect to CLI'.

Access Point	Status	SSIDs	Channel	Health	Clients	OS Version
FP231ETF20000458	Waiting for Authorization	R1 All R2 All R3 N/A	R1 0 R2 0 R3 N/A		0	
PS423E3X16000075	Online	R1 FOS-QA-MelodyZhou-bridge-1 (ssid-bridge) R2 All	R1 11 R2 124	Fair	0	PS423E-v6.4-build0410

3. Click the *VLAN Probe* tab.
  - a. Configure the settings in the *VLAN Range* field.
  - b. Click *Start*.

**FortiGate 81E-POE** FortiGate-81E-POE

Summary of PS423E3X16000075

Serial Number: PS423E3X16000075  
 Base MAC Address: 90:6c:ac:8a:6a:50  
 Status: Connected  
 Country/Region: US  
 Health: Fair  
 Uplink Interface: lan  
 IPv4 Address: 10.2.100.5  
 Uptime: 23h 59m 7s  
 Version: v6.4 build0410

General Health: Fair

- CPU Usage: 3%
- Memory Usage: 15%
- Connection Uptime: 0 days
- lan1: 1.0 Gbps
- lan2: 0 Mbps

5 GHz Health: Good

- Interfering APs: Disabled
- Clients: 0
- Channel Utilization: 1%

VLAN Probe

Probe Retries: 10  
 Timeout: 5 Seconds  
 VLAN Range: 1 To 10

Start

4. After the VLAN probing is complete, the VLAN probing report appears in the summary page.

**FortiGate 81E-POE** FortiGate-81E-POE

Summary of PS423E3X16000075

Serial Number: PS423E3X16000075  
 Base MAC Address: 90:6c:ac:8a:6a:50  
 Status: Connected  
 Country/Region: US  
 Health: Fair  
 Uplink Interface: lan  
 IPv4 Address: 10.2.100.5  
 Uptime: 1d 28s  
 Version: v6.4 build0410

General Health: Fair

- CPU Usage: 3%
- Memory Usage: 15%
- Connection Uptime: 0 days
- lan1: 1.0 Gbps
- lan2: 0 Mbps

5 GHz Health: Good

- Interfering APs: Disabled
- Clients: 0
- Channel Utilization: 1%

VLAN Probe

New Probe | Retry | Completed

VLAN ID	Interface	Available	Subnet	AP Interface
1	vlan0001	Available	10.11.100.1/24	eth0
2	vlan0002	Available	10.22.100.1/24	eth0
3		Not Available		
4		Not Available		
5		Not Available		
6		Not Available		
7		Not Available		

View All | View Available

## CLI

You can use the CLI console in FortiGate and FortiAP to perform a VLAN probe and view the report.

### FortiGate

#### Command syntax:

```
diagnose wireless-controller wlac -c vlan-probe-cmd <FAP Serial Number> <action> <interface ID> <start Vlan ID> <end Vlan ID> <retry> <timeout>
diagnose wireless-controller wlac -c vlan-probe-rpt <FAP Serial Number> <interface ID>
```

Where the value for `action` is:

- 0 — Start
- 1 — Stop

And where the value for `interface ID` is:

- 0 — All Ethernet port(s) of FortiAP
- 1 — The 1st Ethernet port of FortiAP, `eth0`
- 2 — The 2nd Ethernet port of FortiAP, `eth1`, if the hardware exists

#### To perform a VLAN probe in the CLI:

```
FortiGate-81E-POE (vdom1) # diagnose wireless-controller wlac -c vlan-probe-cmd
PS423E3X16000075 0 0 1 4094 2 10

Sending VLAN probe command to PS423E3X16000075: action=start wan-port=1 vlan=[1,4094]
retries=2 timeout=10s
Sending VLAN probe command to PS423E3X16000075: action=start wan-port=2 vlan=[1,4094]
retries=2 timeout=10s
Stop VLAN probing. You don't need to run stop command to get the probing report, only use
it when you want to stop probing.
FortiGate-81E-POE (vdom1) # diag wi wlac -c vlan-probe-cmd PS423E3X16000075 1 0
Sending VLAN probe command to PS423E3X16000075: action=stop wan-port=1
Sending VLAN probe command to PS423E3X16000075: action=stop wan-port=2
```

#### To view the VLAN probe report in the CLI:

```
FortiGate-81E-POE (vdom1) # diagnose wireless-controller wlac -c vlan-probe-rpt
PS423E3X16000075 0
```

VLAN probing status on `eth0`: Done

intf eth0	VLAN_ID=0001	gateway=10.11.100.1/24	probed_at=Wed Jan 16 17:09:48 2019
intf eth0	VLAN_ID=0002	gateway=10.22.100.1/24	probed_at=Wed Jan 16 17:09:48 2019
intf eth0	VLAN_ID=0003	gateway=10.33.100.1/24	probed_at=Wed Jan 16 17:09:48 2019
intf eth0	VLAN_ID=0004	gateway=10.44.100.1/24	probed_at=Wed Jan 16 17:09:48 2019
intf eth0	VLAN_ID=0005	gateway=10.55.100.1/24	probed_at=Wed Jan 16 17:09:48 2019
intf eth0	VLAN_ID=0006	gateway=10.66.100.1/24	probed_at=Wed Jan 16 17:09:48 2019
intf eth0	VLAN_ID=0007	gateway=10.77.100.1/24	probed_at=Wed Jan 16 17:09:48 2019
intf eth0	VLAN_ID=0100	gateway=10.10.20.2/24	probed_at=Wed Jan 16 17:09:49 2019
intf eth0	VLAN_ID=0200	gateway=10.4.100.1/24	probed_at=Wed Jan 16 17:09:48 2019
intf eth0	VLAN_ID=0300	gateway=10.5.100.1/24	probed_at=Wed Jan 16 17:09:49 2019
intf eth0	VLAN_ID=0400	gateway=10.6.100.1/24	probed_at=Wed Jan 16 17:09:49 2019

```

intf eth0  VLAN_ID=0500 gateway=10.7.100.1/24      probed_at=Wed Jan 16 17:09:49 2019
intf eth0  VLAN_ID=0600 gateway=10.9.100.1/24      probed_at=Wed Jan 16 17:09:49 2019
intf eth0  VLAN_ID=1000 gateway=10.10.100.1/24     probed_at=Wed Jan 16 17:09:49 2019
intf eth0  VLAN_ID=2000 gateway=10.20.100.1/24     probed_at=Wed Jan 16 17:09:49 2019
intf eth0  VLAN_ID=3000 gateway=10.30.100.1/24     probed_at=Wed Jan 16 17:09:49 2019
intf eth0  VLAN_ID=4000 gateway=10.40.100.1/24     probed_at=Wed Jan 16 17:09:49 2019

```

VLAN probing status on eth1: Done

## FortiAP

### Command syntax

```

cw_diag -c vlan-probe-cmd <action> <interface ID> <start Vlan ID> <end Vlan ID> <retry> <timeout>
cw_diag -c vlan-probe-rpt

```

Where the value for action is:

- 0 — Start
- 1 — Stop

### To perform a VLAN probe in the CLI:

```

PS423E3X16000075 # cw_diag -c vlan-probe-cmd 0 eth0 1 4094 2 10
VLAN probing: start intf [eth0] vlan range[1,4094] retries[2] timeout[10s] ...

```

Stop VLAN probing. You don't need to run stop command to get the probing report, only use it when you want to stop probing.

```

PS423E3X16000075 # cw_diag -c vlan-probe-cmd 1 eth0
VLAN probing: stop intf [eth0] vlan range[0,0] retries[0] timeout[0s] ...

```

### To view the VLAN probe report in the CLI:

```

PS423E3X16000075 # cw_diag -c vlan-probe-rpt

```

WTP VLAN probing status: Idle

VLAN probing report on intf[eth0] vlan range[1,4094] retries[2] timeout[10]:

```

VLAN_ID=0001 gateway=10.11.100.1/24 age=289
VLAN_ID=0002 gateway=10.22.100.1/24 age=289
VLAN_ID=0003 gateway=10.33.100.1/24 age=289
VLAN_ID=0004 gateway=10.44.100.1/24 age=289
VLAN_ID=0005 gateway=10.55.100.1/24 age=289
VLAN_ID=0006 gateway=10.66.100.1/24 age=289
VLAN_ID=0007 gateway=10.77.100.1/24 age=289
VLAN_ID=0100 gateway=10.3.100.1/24 age=289
VLAN_ID=0200 gateway=10.4.100.1/24 age=289
VLAN_ID=0300 gateway=10.5.100.1/24 age=289
VLAN_ID=0400 gateway=10.6.100.1/24 age=289
VLAN_ID=0500 gateway=10.7.100.1/24 age=289
VLAN_ID=0600 gateway=10.9.100.1/24 age=289
VLAN_ID=1000 gateway=10.10.100.1/24 age=289
VLAN_ID=2000 gateway=10.20.100.1/24 age=289
VLAN_ID=3000 gateway=10.30.100.1/24 age=289

```



```
VLAN_ID=4000 gateway=10.40.100.1/24 age=289
```

```
VLAN probing report on intf[eth1] vlan range[1,4094] retries[2] timeout[10]:
```

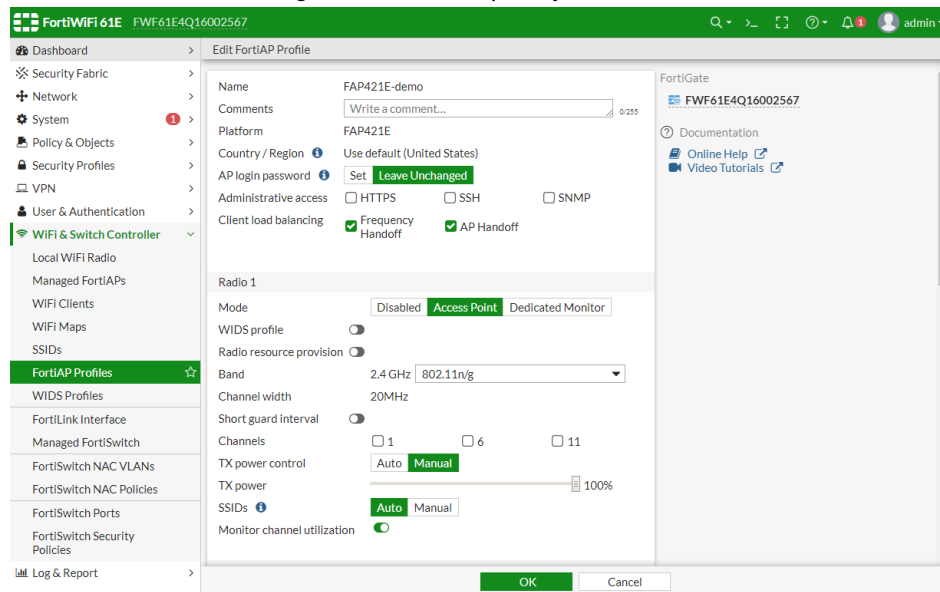
## FortiAP client load balancing per AP

The frequency and AP handoff options are moved from the radio level to the global section of FortiAP profiles. If either load balancing options are enabled on any radio prior to upgrading, the setting will be enabled after upgrading.

In this example, a new custom profile is created with both client load balancing options are enabled.

### To configure a custom AP profile in the GUI:

1. Go to *WiFi & Switch Controller > FortiAP Profiles*.
2. Click *Create New* or edit an existing custom profile.
3. In the *Client load balancing* field, select *Frequency Handoff* and *AP Handoff*.



4. Configure the remaining settings as required.
5. Click **OK**.

### To configure a custom AP profile in the CLI:

```
config wireless-controller wtp-profile
  edit "FAP421E-demo"
    config platform
      set type 421E
    end
    set handoff-sta-thresh 55
    set frequency-handoff enable
    set ap-handoff enable
  config radio-1
    set band 802.11n,g-only
  end
  config radio-2
```

```

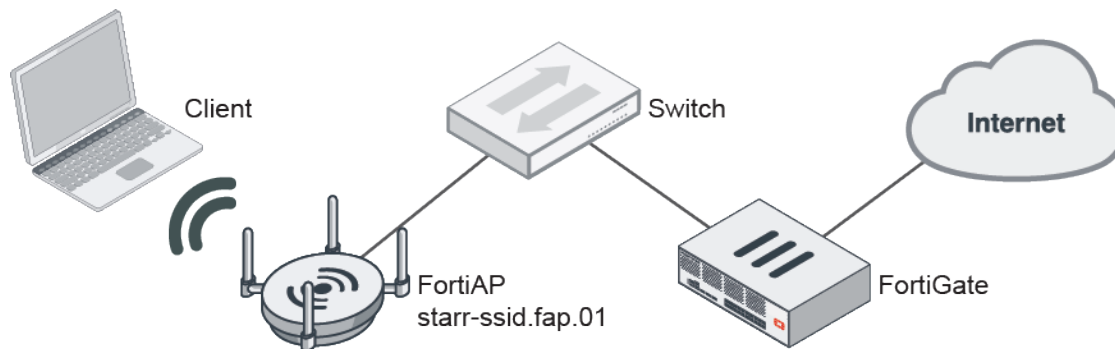
        set band 802.11ac
    end
next
end

```

## Layer three ACL configurations for Wireless APs

For FortiAP devices (6.4.0 and later) that are managed by FortiGate, a layer three (L3) access control list (ACL) can be applied to a bridge or tunnel mode SSID.

### Example



In this example:

- Rule 10 is to block all traffic to 172.16.200.44
- Rule 20 is to block all ICMP traffic
- Rule 30 is to block traffic to destination port 21 (FTP)

### To configure L3 ACL:

#### 1. Create L3 firewall rules:

```

config wireless-controller access-control-list
  edit "ACL-1"
    config layer3-ipv4-rules
      edit 10
        set dstaddr 172.16.200.44/255.255.255.255
        set action deny
      next
      edit 20
        set protocol 1
        set action deny
      next
      edit 30
        set dstport 21
        set action deny
      next
    end
  next
end

```

**2. Apply the rules to VAP:**

```
config wireless-controller vap
  edit "wifi.fap.01"
    set ssid "starr-ssid.fap.01"
    set passphrase *****
    set local-bridging enable
    set access-control-list "ACL-1"
  next
end
```

**3. Check the rules on the FortiGate:**

```
# diagnose wireless-controller wlac -c afwprof

AFWPROF (001/001) vdom,name: vdom1, ACL-1
  refcnt      : 2 own(1) wlan(1)
  deleted     : no
  Layer3 ipv4 rule : 3

-----
##### Policy Prot Source ==> Destination
-----
  10 deny    any  any:any ==> 172.16.200.44/32:any
  20 deny    1    any:any ==> any:any
  30 deny    any  any:any ==> any:21
-----

wlan cnt      : 1
vap 001 : 1    wifi.fap.01
```

**4. Confirm that the L3 rules are pushed to the FortiAP:**

```
# cw_diag -c afw-rules

Interface wlan00 firewall rules:
=====
RuleID HitCounter Policy Prot (IPv4)Source ==> Destination
-----
  10          0 deny    any  any:any ==> 172.16.200.44/32:any
  20          0 deny    1    any:any ==> any:any
  30          0 deny    any  any:any ==> any:21
=====
```

**5. On the client, confirm that the rules are applied:****a. Rule 10: Traffic to 172.16.200.44 is blocked, and traffic to other destinations are allowed:**

```
root@pc_wifi:~# curl 172.16.200.44 -v
* Rebuilt URL to: 172.16.200.44/
* Trying 172.16.200.44...
* connect to 172.16.200.44 port 80 failed: Connection timed out
* Failed to connect to 172.16.200.44 port 80: Connection timed out
* Closing connection 0
curl: (7) Failed to connect to 172.16.200.44 port 80: Connection timed out
root@pc_wifi:~#

root@pc_wifi:~# curl -k https://172.18.56.163
<html><body><h1>It works!</h1>
<p>This is the default web page for this server-44.</p>
<p>The web server software is running but no content has been added, yet. Managed by
Starr Q</p>
```

**b. Rule 20: ICMP traffic is blocked and HTTPS traffic is allowed:**

```
root@pc_wifi:~# ping 172.16.200.44
PING 172.16.200.44 (172.16.200.44) 56(84) bytes of data.
^C
--- 172.16.200.44 ping statistics ---
86 packets transmitted, 0 received, 100% packet loss, time 85680ms

root@pc_wifi:~# curl -k https://172.18.56.163
<html><body><h1>It works!</h1>
<p>This is the default web page for this server-44.</p>
<p>The web server software is running but no content has been added, yet. Managed by
Starr Q</p>
```

**c. Rule 30: FTP traffic is blocked:**

```
oot@pc_wifi:~# ftp 172.18.56.163
ftp: connect: Connection timed out
ftp> ^C
ftp> bye
```

## Maintain radio SSID WLAN IDs

WLAN IDs remain the same after a daemon restart or a controller reboot. BSSIDs also remain the same, which keeps the WiFi service stable. This is confirmed by read-only commands in the downloaded backup FortiOS configuration file and the `iwconfig` output from FortiAP.

### Sample FortiOS configuration

```
config wireless-controller vap
  edit "wifi-m-1"
    set mesh-backhaul enable
    set ssid "FOS-QA-LFU-FWF61E-M-1"
    set broadcast-ssid disable
    set passphrase qa12345678
    set schedule "always"
  next
  edit "wifi-b-1"
    set ssid "FOS-QA-LFU-FWF61E-B-2"
    set passphrase qa12345678
    set local-bridging enable
    set schedule "always"
  next
  edit "wifi-b-2"
    set ssid "FOS-QA-LFU-FWF61E-B-2"
    set passphrase qa12345678
    set local-bridging enable
    set schedule "always"
  next
  edit "wifi-b-3"
    set ssid "FOS-QA-LFU-FWF61E-B-3"
    set passphrase qa12345678
    set local-bridging enable
    set schedule "always"
  next
```

```
edit "wifi-b-4"
    set ssid "FOS-QA-LFU-FWF61E-B-4"
    set passphrase qa12345678
    set local-bridging enable
    set schedule "always"
next
edit "wifi-b-5"
    set ssid "FOS-QA-LFU-FWF61E-B-5"
    set passphrase qa12345678
    set local-bridging enable
    set schedule "always"
next
edit "wifi-b-6"
    set ssid "FOS-QA-LFU-FWF61E-B-6"
    set passphrase qa12345678
    set local-bridging enable
    set schedule "always"
next
end
```

### Backup configuration file output

#### To verify that the SSIDs remain the same:

```
config wireless-controller wtp-profile
edit "FAP423E-default"
    config platform
        set type 423E
    end
    set handoff-sta-thresh 30
    set allowaccess https ssh snmp
    config radio-1
        set band 802.11n,g-only
        set channel-utilization disable
        set vap-all none
    end
    config radio-2
        set band 802.11ac
        set channel-utilization disable
        set darp enable
        set vap-all none
        set vaps "wifi-b-1" "wifi-b-2" "wifi-b-3" "wifi-b-4" "wifi-b-5" "wifi-b-6"
"wifi-m-1"
    set vap1 "wifi-b-1"
    set vap2 "wifi-b-2"
    set vap3 "wifi-b-3"
    set vap4 "wifi-b-4"
    set vap5 "wifi-b-5"
    set vap6 "wifi-b-6"
    set vap7 "wifi-m-1"
    end
    set ext-info-enable disable
next
end
```

```
cconfig wireless-controller wtp
  edit "FP423E3X16000320"
    set admin enable
    set wtp-profile "FAP423E-default"
    config radio-1
      set override-vaps enable
      set vap-all none
      set vaps "wifi-b-1" "wifi-b-2" "wifi-b-3" "wifi-b-4" "wifi-b-5" "wifi-b-6"
      "wifi-m-1"
        set vap1 "wifi-b-1"
        set vap2 "wifi-b-2"
        set vap3 "wifi-b-3"
        set vap4 "wifi-b-4"
        set vap5 "wifi-b-5"
        set vap6 "wifi-b-6"
        set vap7 "wifi-m-1"
      end
    config radio-2
    end
  next
end
```

### FortiAP iwconfig output

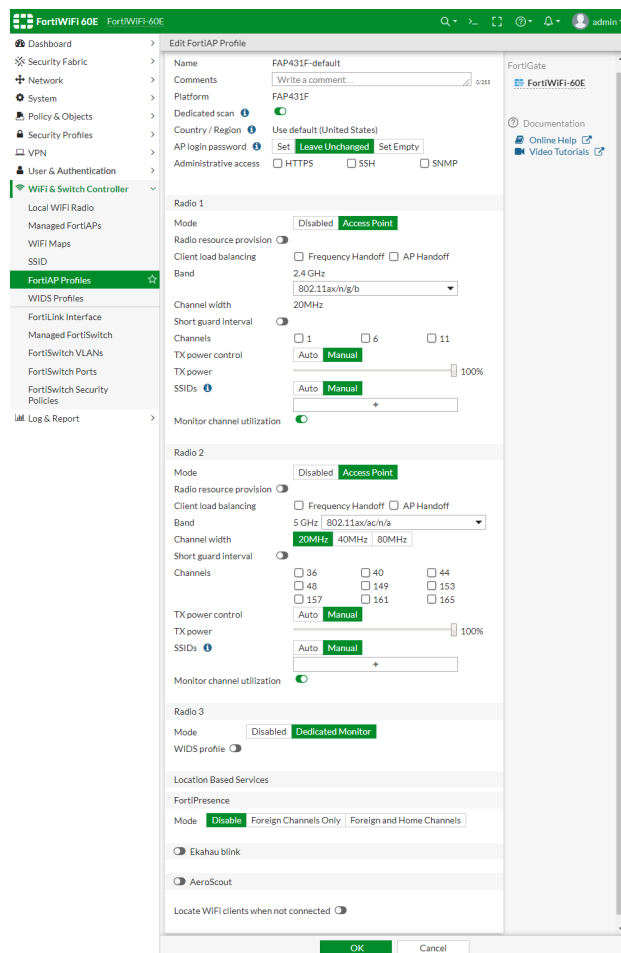
Verify the `iwconfig` output before and after a reboot to confirm that the BSSIDs remain the same. The AP MAC addresses and WLAN IDs will be the same after the reboot.

## Support for FAP431F and FAP433F

FortiOS 6.4 supports FortiAP NPI models FAP431F and FAP433F. You can use the GUI or CLI to create and edit WTP profiles for platform types 431F and 433F.

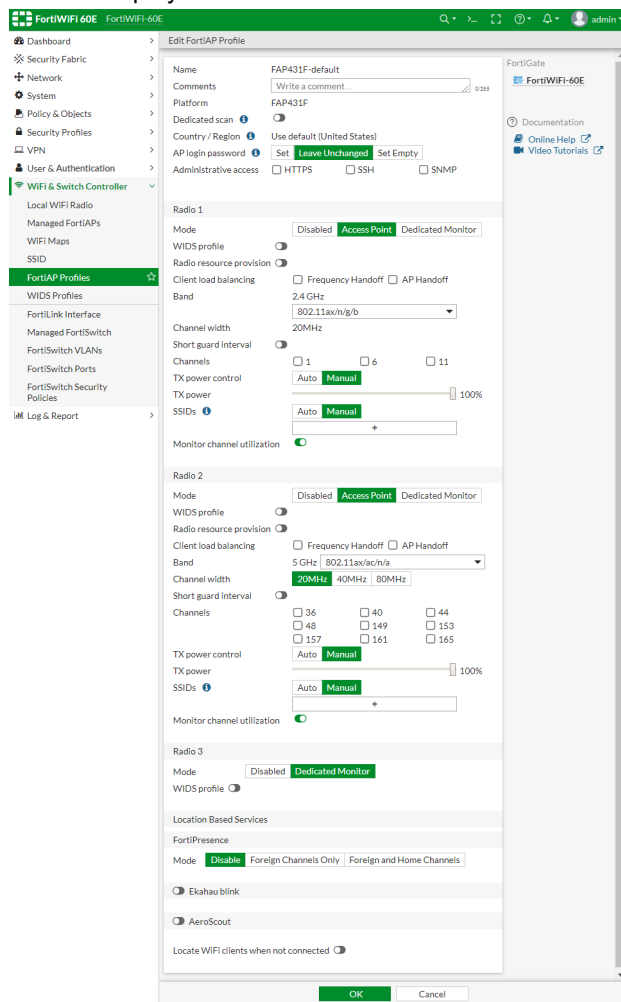
### To view the default configuration with the GUI:

1. Go to *Wifi & Switch Controller > FortiAP Profiles*, and click *Create New*. The *New FortiAP Profile* window opens.
2. From the *Platform* dropdown, select *FAP431F* or *FAP433F*. The default profile opens.
  - *Dedicated scan* is enabled by default.
  - Radio 1 and Radio 2 display *Disabled* and *Access Point* mode.
  - Radio 3 displays *Disabled* and *Dedicated Monitor* mode.



3. Disable *Dedicated Scan*.  
When *Dedicated Scan* is disabled:

- Radio 1 and Radio 2 display *Disabled*, *Access Point*, and *Dedicated Monitor* mode.
- Radio 3 displays *Disabled* and *Dedicated Monitor* mode.



## Sample CLI configurations

### FAP43xF models support 802.11ax on both 2.4G and 5G radios

```
FortiWiFi-60E # config wireless-controller wtp-profile
FortiWiFi-60E (wtp-profile) # ed FAP431F-default
FortiWiFi-60E (FAP431F-default) # conf radio-1
FortiWiFi-60E (radio-1) # set band ?
802.11b                802.11b.
802.11g                802.11g/b.
802.11n                802.11n/g/b at 2.4GHz.
802.11ax              802.11ax/n/g/b at 2.4GHz.
802.11n,g-only        802.11n/g at 2.4GHz.
802.11g-only          802.11g.
802.11n-only          802.11n at 2.4GHz.
802.11ax,n-only       802.11ax/n at 2.4GHz.
802.11ax,n,g-only     802.11ax/n/g at 2.4GHz.
802.11ax-only         802.11ax at 2.4GHz.
```



```
FortiWiFi-60E (radio-1) # en
FortiWiFi-60E (FAP431F-default) # conf radio-2
FortiWiFi-60E (radio-2) # set band ?
802.11a                802.11a.
802.11n-5G             802.11n/a at 5GHz.
802.11ac               802.11ac/n/a.
802.11ax-5G            802.11ax/ac/n/a at 5GHz.
802.11n-5G-only        802.11n at 5GHz.
802.11ac,n-only        802.11ac/n.
802.11ac-only          802.11ac.
802.11ax,ac-only       802.11ax/ac at 5GHz.
802.11ax,ac,n-only     802.11ax/ac/n at 5GHz.
802.11ax-5G-only       802.11ax at 5GHz.

FortiWiFi-60E (radio-2) # en
FortiWiFi-60E (FAP431F-default) #
```

### **ddscan is enabled by default when creating a new profile for FAP43xF models**

```
FortiWiFi-60E # config wireless-controller wtp-profile
FortiWiFi-60E (wtp-profile) # ed 431F
new entry '431F' added
FortiWiFi-60E (431F) # conf platform
FortiWiFi-60E (platform) # set type 431F
FortiWiFi-60E (platform) # sh
config platform
    set type 431F
    set ddscan enable
end
FortiWiFi-60E (platform) # en
FortiWiFi-60E (431F) # sh
config wireless-controller wtp-profile
    edit "431F"
        config platform
            set type 431F
            set ddscan enable
        end
        set handoff-sta-thresh 55
        config radio-1
            set band 802.11ax
        end
        config radio-2
            set band 802.11ax-5G
        end
        config radio-3
            set mode monitor
        end
    next
end
FortiWiFi-60E (431F) # en
```

### **Radio 3 of FAP43xF models will only support monitor, sniffer, and disable mode when ddscan is enabled or disabled**

When ddscan is enabled:

```
FortiWiFi-60E # config wireless-controller wtp-profile
```

```

FortiWiFi-60E (wtp-profile) # ed 431F
FortiWiFi-60E (431F) # conf platform
FortiWiFi-60E (platform) # set ddscan enable
FortiWiFi-60E (platform) # end
FortiWiFi-60E (431F) # conf radio-3
FortiWiFi-60E (radio-3) # set mode
disabled      Radio 3 is disabled.
monitor       Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other
              WiFi access points and adds them to the Rogue AP monitor list.
sniffer       Radio 3 operates as a sniffer capturing WiFi frames on air.

FortiWiFi-60E (radio-3) # set mode monitor
FortiWiFi-60E (radio-3) # end
FortiWiFi-60E (431F) # end

```

#### When ddscan is disabled:

```

FortiWiFi-60E # config wireless-controller wtp-profile
FortiWiFi-60E (wtp-profile) # ed 431F
FortiWiFi-60E (431F) # conf platform
FortiWiFi-60E (platform) # set ddscan disable
FortiWiFi-60E (platform) # end
FortiWiFi-60E (431F) # conf radio-3
FortiWiFi-60E (radio-3) # set mode
disabled      Radio 3 is disabled.
monitor       Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other
              WiFi access points and adds them to the Rogue AP monitor list.
sniffer       Radio 3 operates as a sniffer capturing WiFi frames on air.

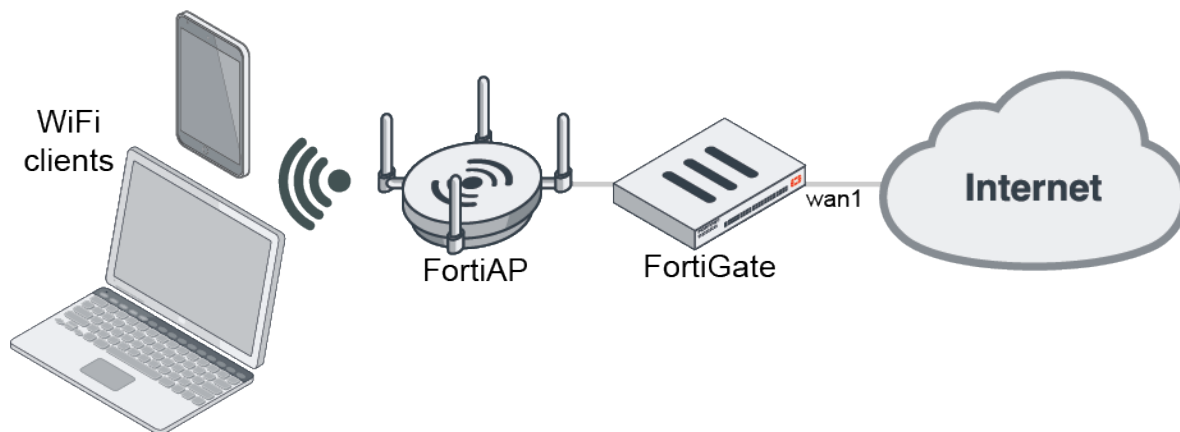
FortiWiFi-60E (radio-3) # set mode monitor
FortiWiFi-60E (radio-3) # end
FortiWiFi-60E (431F) # end

```

## Support logging the signal-to-noise ratio and signal strength per client - 6.4.1

The signal-to-noise ratio (`snr`) and signal strength (`signal`) are logged per client in the WiFi event and traffic logs.

When a WiFi client connects to a tunnel or local-bridge mode SSID on an FortiAP that is managed by a FortiGate, signal-to-noise ratio and signal strength details are included in WiFi event logs for local-bridge traffic statistics and authentication, and in forward traffic logs for tunnel traffic. This allows you to store and view clients' historical signal strength and signal-to-noise ratio information.



## To verify when a client is connecting to an SSID:

1. Go to **Log & Report > Events** and select **WiFi Events** from the events drop-down list.

The **Signal** and **Signal/Noise** columns show the signal strength and signal-to-noise ratio for each applicable client.

Add Filter				WiFi Events		Details	
Date/Time	Level	Action	Message	SSID	Channel	Signal	Signal/Noise
2020/05/29 10:00:16	<div><div></div></div>	fake-ap-on-air	Fake AP On-air starr-ssid.fap.02 90:6c:ac:8a:69:41 chan 44 live ...	starr-ssid.fap.02	44	-34	
2020/05/29 10:00:15	<div><div></div></div>	DHCP-ACK	DHCP ACK for IP 11.10.80.2 from server 11.10.80.1 for client 4...	FOS_QA_Starr_140E_Guest-11			
2020/05/29 10:00:15	<div><div></div></div>	DHCP-REQUEST	DHCP REQUEST for IP 11.10.80.2 offered by server 11.10.80.1 ...	FOS_QA_Starr_140E_Guest-11			
2020/05/29 10:00:15	<div><div></div></div>	DHCP-OFFER	DHCP OFFER of IP 11.10.80.2 from server 11.10.80.1 for client ...	FOS_QA_Starr_140E_Guest-11			
2020/05/29 10:00:14	<div><div></div></div>	client-ip-detected	Client 48:ee:0c:23:43:d1 had an IP address detected (by DHCP ...	FOS_QA_Starr_140E_Guest-11	6	-45	50
2020/05/29 10:00:14	<div><div></div></div>	DHCP-DISCOVER	DHCP DISCOVER from client 48:ee:0c:23:43:d1	FOS_QA_Starr_140E_Guest-11			
2020/05/29 10:00:04	<div><div></div></div>	client-authentication	Client 48:ee:0c:23:43:d1 authenticated.	FOS_QA_Starr_140E_Guest-11	6	-45	50
2020/05/29 10:00:04	<div><div></div></div>	WPA-4/4-key-msg	AP received 4/4 message of 4-way handshake from client 48:ee...	FOS_QA_Starr_140E_Guest-11	6		
2020/05/29 10:00:04	<div><div></div></div>	WPA-3/4-key-msg	AP sent 3/4 message of 4-way handshake to client 48:ee:0c:23...	FOS_QA_Starr_140E_Guest-11	6		
2020/05/29 10:00:04	<div><div></div></div>	WPA-2/4-key-msg	AP received 2/4 message of 4-way handshake from client 48:ee...	FOS_QA_Starr_140E_Guest-11	6		
2020/05/29 10:00:04	<div><div></div></div>	WPA-1/4-key-msg	AP sent 1/4 message of 4-way handshake to client 48:ee:0c:23...	FOS_QA_Starr_140E_Guest-11	6		
2020/05/29 10:00:04	<div><div></div></div>	assoc-resp	AP sent association response frame to client 48:ee:0c:23:43:d1	FOS_QA_Starr_140E_Guest-11	6		
2020/05/29 10:00:04	<div><div></div></div>	assoc-req	AP received association request frame from client 48:ee:0c:23:4...	FOS_QA_Starr_140E_Guest-11	6		
2020/05/29 10:00:04	<div><div></div></div>	auth-resp	AP sent authentication response frame to client 48:ee:0c:23:43...	FOS_QA_Starr_140E_Guest-11	6		
2020/05/29 10:00:04	<div><div></div></div>	auth-req	AP received authentication request frame from client 48:ee:0c:...	FOS_QA_Starr_140E_Guest-11	6		
2020/05/29 09:59:30	<div><div></div></div>	oper-tpxpower	AP FP231ETF20000455 radio 1 oper tpxpower is changed to 26 ...				
2020/05/29 09:59:28	<div><div></div></div>	oper-tpxpower	AP FP231ETF20000455 radio 1 oper tpxpower is changed to 4 d...				
2020/05/29 09:59:24	<div><div></div></div>	config-tpxpower	AP FP231ETF20000455 radio 1 cfg tpxpower is changed to 27 d...				
2020/05/29 09:58:46	<div><div></div></div>	fake-ap-on-air	Fake AP On-air starr-ssid.fap.02 90:6c:ac:8a:69:41 chan 44 live ...	starr-ssid.fap.02	44	-34	
2020/05/29 09:57:16	<div><div></div></div>	fake-ap-on-air	Fake AP On-air starr-ssid.fap.02 90:6c:ac:8a:69:41 chan 44 live ...	starr-ssid.fap.02	44	-34	
2020/05/29 09:55:46	<div><div></div></div>	fake-ap-on-air	Fake AP On-air starr-ssid.fap.02 90:6c:ac:8a:69:41 chan 44 live ...	starr-ssid.fap.02	44	-34	0% 108

2. WiFi event log messages include the signal and snr values:

```
date=2020-05-27 time=11:26:28 logid="0104043579" type="event" subtype="wireless"
level="notice" vd="vdom1" eventtime=1590603988877156921 tz="-0700" logdesc="Wireless
client IP assigned" sn="FP231ETF20000455" ap="FP231ETF20000455" vap="stability3"
ssid="FOS_QA_Starr_140E_Guest-11" radioid=1 user="N/A" group="N/A"
stamac="1c:87:2c:b6:a8:49" srcip=11.10.80.2 channel=6 radioband="802.11n,g-only"
signal=-45 snr=50 security="WPA2 Personal" encryption="AES" action="client-ip-detected"
reason="Reserved 0" mpsk="N/A" msg="Client 1c:87:2c:b6:a8:49 had an IP address detected
(by DHCP packets)."
```

```
date=2020-05-27 time=11:26:11 logid="0104043573" type="event" subtype="wireless"
level="notice" vd="vdom1" eventtime=1590603970962702892 tz="-0700" logdesc="Wireless
client authenticated" sn="FP231ETF20000455" ap="FP231ETF20000455" vap="stability3"
ssid="FOS_QA_Starr_140E_Guest-11" radioid=1 user="N/A" group="N/A"
stamac="1c:87:2c:b6:a8:49" srcip=0.0.0.0 channel=6 radioband="802.11n,g-only" signal=-45
snr=50 security="WPA2 Personal" encryption="AES" action="client-authentication"
reason="Reserved 0" mpsk="N/A" msg="Client 1c:87:2c:b6:a8:49 authenticated."
```

## To verify tunnel traffic when a client is connecting to a tunnel mode SSID:

1. Go to **Log & Report > Forward Traffic**.

The **Signal** and **Signal/Noise** columns show the signal strength and signal-to-noise ratio for each applicable client.

Add Filter										55	Details
Date/Time		Source	Device	Destination	Application Name	Result	Policy ID	Signal	Signal/Noise		
2020/05/29 10:19:04		11.10.80.3	00:1e:e5:df:b1:63	108.175.12.139 (img2.westca.com)	HTTPS.BROWSER	✓ 938 B / 389 B	wmm (13)	-32	62		
2020/05/29 10:19:04		11.10.80.3	00:1e:e5:df:b1:63	108.175.12.139 (img2.westca.com)	HTTPS.BROWSER	✓ 938 B / 389 B	wmm (13)	-32	62		
2020/05/29 10:19:02		11.10.80.6	WIFI23	142.232.230.11 (www.bclt.ca)	SSL_TLSv1.2	✓ 3.67 kB / 97.47 kB	wmm (13)	-30	64		
2020/05/29 10:18:58		11.10.80.3	00:1e:e5:df:b1:63	108.175.12.139 (img2.westca.com)	HTTPS.BROWSER	✓ 938 B / 389 B	wmm (13)	-32	62		
2020/05/29 10:18:51		11.10.80.3	00:1e:e5:df:b1:63	149.7.32.209 (widgetdata-backup.tradingview.com)	SSL_TLSv1.2	✓ 255.25 kB / 903.92 kB	wmm (13)	-32	62		
2020/05/29 10:18:46		11.10.80.3	00:1e:e5:df:b1:63	108.175.12.139 (img2.westca.com)	HTTPS.BROWSER	✓ 938 B / 389 B	wmm (13)	-34	60		
2020/05/29 10:18:46		11.10.80.6	WIFI23	172.18.56.163	HTTP.BROWSER	✓ 397 B / 669 B	wmm (13)	-30	64		
2020/05/29 10:18:35		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 59 B / 292 B	wmm (13)	-34	60		
2020/05/29 10:18:35		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 63 B / 240 B	wmm (13)	-34	60		
2020/05/29 10:18:35		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 59 B / 166 B	wmm (13)	-34	60		
2020/05/29 10:18:35		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 59 B / 292 B	wmm (13)	-34	60		
2020/05/29 10:18:35		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 59 B / 292 B	wmm (13)	-34	60		
2020/05/29 10:18:35		11.10.80.3	00:1e:e5:df:b1:63	65.39.243.196 (www.everforx.ca)	HTTPS.BROWSER	✓ 596.72 kB / 2.97 MB	wmm (13)	-34	60		
2020/05/29 10:18:34		11.10.80.3	00:1e:e5:df:b1:63	108.175.12.139 (img2.westca.com)	HTTPS.BROWSER	✓ 936 B / 429 B	wmm (13)	-34	60		
2020/05/29 10:18:32		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 79 B / 243 B	wmm (13)	-34	60		
2020/05/29 10:18:32		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 79 B / 243 B	wmm (13)	-34	60		
2020/05/29 10:18:32		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 59 B / 267 B	wmm (13)	-34	60		
2020/05/29 10:18:32		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 59 B / 157 B	wmm (13)	-34	60		
2020/05/29 10:18:31		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 59 B / 267 B	wmm (13)	-34	60		
2020/05/29 10:18:31		11.10.80.3	00:1e:e5:df:b1:63	172.16.100.100	DNS	✓ 59 B / 267 B	wmm (13)	-34	60		

## 2. Forward traffic log messages include the signal and snr values:

```
date=2020-05-27 time=11:30:26 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1590604226533016978 tz="-0700" srcip=11.10.80.2
srcname="WIFI23" srcport=53926 srcintf="stability3" srcintfrole="lan" srcssid="FOS_QA_
Starr_140E_Guest-11" apsn="FP231ETF20000455" ap="FP231ETF20000455" channel=6
radioband="802.11n,g-only" signal=-31 snr=64 dstip=91.189.91.157 dstport=123
dstintf="wan1" dstintfrole="wan" srccountry="United States" dstcountry="United States"
sessionid=322069 proto=17 action="accept" policyid=13 policytype="policy"
poluuid="7c14770c-1456-51e9-4c57-806e9c499782" policyname="wmm" service="NTP"
trandisp="snat" transip=172.16.200.111 transport=53926 appid=16270 app="NTP"
appcat="Network.Service" apprisk="elevated" applist="g-default" duration=180 sentbyte=76
rcvdbyte=76 sentpkt=1 rcvpkt=1 utmaction="allow" countapp=1 osname="Linux"
mastersrcmac="1c:87:2c:b6:a8:49" srcmac="1c:87:2c:b6:a8:49" srcserver=0 utmref=65534-66
```

## To verify local-bridge traffic statistics when a client is connecting to a local-bridge mode SSID:

### 1. Go to *Log & Report > Events* and select *WiFi Events* from the events drop-down list.

The *Signal* and *Signal/Noise* columns show the signal strength and signal-to-noise ratio for each applicable client.

Action: sta-wl-bridge-traffic-stats										Add Filter		WiFi Events		55%		Details	
Date/Time	Level	Action	Message			SSID	Channel	Signal	Signal/Noise								
2020/05/29 10:44:44	<div><div></div></div>	sta-wl-bridge-traffic-stats	Traffic stats for bridge ssid client 00:1e:e5:df:b1:63			FOS_QA_Starr-140E-LB		-53	51								
2020/05/29 10:39:44	<div><div></div></div>	sta-wl-bridge-traffic-stats	Traffic stats for bridge ssid client 00:1e:e5:df:b1:63			FOS_QA_Starr-140E-LB		-54	50								
2020/05/29 10:34:44	<div><div></div></div>	sta-wl-bridge-traffic-stats	Traffic stats for bridge ssid client 00:1e:e5:df:b1:63			FOS_QA_Starr-140E-LB		-54	51								
2020/05/29 10:29:44	<div><div></div></div>	sta-wl-bridge-traffic-stats	Traffic stats for bridge ssid client 00:1e:e5:df:b1:63			FOS_QA_Starr-140E-LB		-52	52								

### 2. WiFi event log messages include the signal and snr values:

```
date=2020-05-26 time=17:48:57 logid="0104043687" type="event" subtype="wireless"
level="information" vd="vdom1" eventtime=1590540537841497433 tz="-0700" logdesc="Traffic
stats for station with bridge wlan" sn="FP231ETF20000455" ap="FP231ETF20000455"
vap="wifi.fap.01" ssid="FOS_QA_Starr-140E-LB-cap-2" srcip=10.128.100.4 user="N/A"
stamac="00:1e:e5:df:b1:63" signal=-53 snr=52 sentbyte=8970016 rcvdbyte=985910
nextstat=300 action="sta-wl-bridge-traffic-stats" msg="Traffic stats for bridge ssid
client 00:1e:e5:df:b1:63"
```

## Simplify BLE profiles to support broadcast of FortiAP UUID - 6.4.2

Each Bluetooth Low Energy (BLE) profile broadcasts a unique iBeacon UUID. The BLE profile can now be used to broadcast a unique beacon per FortiAP.

A new CLI read-only string, `wtp-uuid`, for the `ibeacon uuid` option is added to automatically generate UUIDs based on the serial number of the FortiAP.

The following default BLE profile, `fortiap-discovery`, is available in FortiOS:

```
config wireless-controller ble-profile
  edit "fortiap-discovery"
    set advertising ibeacon eddystone-uuid eddystone-url
    set ibeacon-uuid "wtp-uuid"
  next
end
```

### To configure the BLE profile:

```
config wireless-controller ble-profile
  edit "test_new_feature"
    set comment "QAdoc"
    set advertising ibeacon eddystone-uuid eddystone-url
    set ibeacon-uuid "wtp-uuid"
    set major-id 65535
    set minor-id 65535
    set eddystone-namespace "test"
    set eddystone-instance "test"
    set eddystone-url "https://www.test.com"
    set txpower 5
    set beacon-interval 45
    set ble-scanning enable
  next
end
```

### To apply the BLE profile to a WTP profile:

```
config wireless-controller wtp-profile
  edit "FAPU321EV-default"
    config platform
      set type U321EV
    end
    set ble-profile "test_new_feature"
    set handoff-sta-thresh 30
    set allowaccess https ssh snmp
    set frequency-handoff enable
    set ap-handoff enable
    config radio-1
      set band 802.11n,g-only
    end
    config radio-2
      set band 802.11ac
    end
    set ext-info-enable disable
  next
end
```

### To view the BLE profile on the FortiGate:

```
# diagnose wireless-controller wlac -c bleprof
BLEPROF (002/010) vdom,name: root, test_new_feature
```

```
refcnt          : 2 own(1) wtpprof(1)
deleted         : no
advertising     : ibeacon eddystone-uid eddystone-url
ibeacon_uuid   : wtp-uuid
major ID       : 65535
minor ID       : 65535
eddystone namespace ID : test
eddystone instance ID : test
eddystone URL   : https://www.test.com
txpower        : level (5) dBm (-6)
beacon interval : 45
BLE scanning    : enabled
wtpprof cnt     : 1
wtpprof 001    : FAPU321EV-default
```

### To view the BLE profile on the FortiAP:

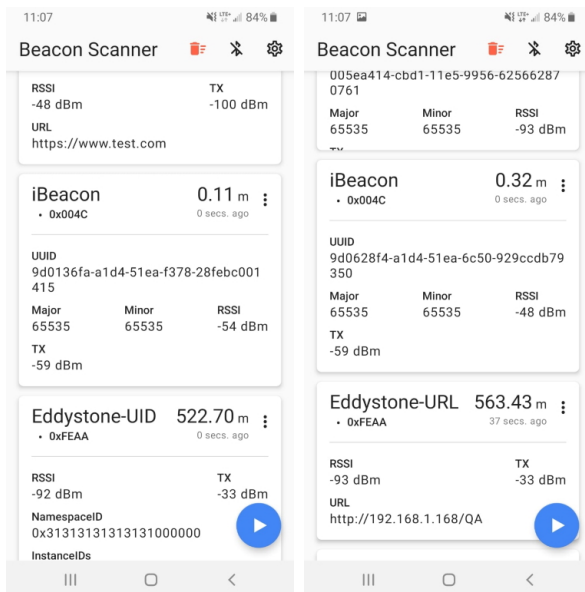
```
# cw_diag -c ble-config
WTP Bluetooth Low Energy Configuration:
  ble scan report interval : 35
  advertising              : ibeacon eddystone-uid eddystone-url
  ibeacon_uuid             : 9d0136fa-a1d4-51ea-f378-28febc001415
  major ID                 : 65535
  minor ID                 : 65535
  eddystone namespace ID   : test
  eddystone instance ID    : test
  eddystone URL            : https://www.test.com
  txpower                  : 5
  beacon interval          : 45
  ble scanning             : enabled
```

BLE address: 00:0c:e6:67:2e:b1

```
# cw_diag -c ble-config
WTP Bluetooth Low Energy Configuration:
  ble scan report interval : 35
  advertising              : ibeacon eddystone-uid eddystone-url
  ibeacon_uuid             : 9d0628f4-a1d4-51ea-6c50-929ccdb79350
  major ID                 : 65535
  minor ID                 : 65535
  eddystone namespace ID   : test
  eddystone instance ID    : test
  eddystone URL            : https://www.test.com
  txpower                  : 5
  beacon interval          : 45
  ble scanning             : enabled
```

BLE address: 00:0c:e6:66:c4:91

The following output from the Beacon Scanner app shows details for both APs, including the iBeacon UUIDs:



## Add ARP profile for wireless controller - 6.4.2

The ARP (Automatic Radio Resource Provisioning) profile improves upon DARRP (Distributed Automatic Radio Resource Provisioning) by allowing more factors to be considered to optimize channel selection among FortiAPs. DARRP uses the neighbor APs channels and signal strength collected from the background scan for channel selection.

### To configure the ARP profile in FortiOS:

#### 1. Create the ARP profile:

```
config wireless-controller arrp-profile
  edit "arrp-default"
    set comment ''
    set selection-period 3600
    set monitor-period 300
    set weight-managed-ap 50
    set weight-rogue-ap 10
    set weight-noise-floor 40
    set weight-channel-load 20
    set weight-spectral-rssi 40
    set weight-weather-channel 1000
    set weight-dfs-channel 500
    set threshold-ap 250
    set threshold-noise-floor "-85"
    set threshold-channel-load 60
    set threshold-spectral-rssi "-65"
    set threshold-tx-retries 300
    set threshold-rx-errors 50
    set include-weather-channel no
    set include-dfs-channel no
  next
end
```

**2. Enable the DARRP option in the radio configuration:**

```

config wireless-controller wtp-profile
  edit "S421E"
    config platform
      set type S421E
    end
    config radio-1
      set darrp enable
    end
    config radio-2
      set darrp enable
    end
  next
end

```

**3. Configure the DARRP optimize time and schedule:**

```

config wireless-controller setting
  set darrp-optimize 300
  set darrp-optimize-schedules "sche-darrp"
end

```

**To view the ARRP profile and verify the DARRP function in FortiAP:**

```
# cw_diag -c darrp
```

```
Radio 0 Darrp yes
```

```

  selection period      : 3600 sec
  monitor   period      : 300 sec

```

```

  weight-managed-ap      : 50
  weight-rogue-ap        : 10
  weight-noise-floor      : 40
  weight-channel-load     : 20
  weight-weather-channel  : 1000
  weight-dfs-channel      : 500

```

```

  threshold-ap           : 250
  threshold-noise-floor   : -85 dBm
  threshold-channel-load  : 40
  threshold-spectral-rssi : -65 dBm
  threshold-tx-retries    : 300%
  threshold-rx-errors     : 50%
  include-weather-channel : 0
  include-dfs-channel     : 0

```

		chan_load(%)				noise_floor(dBm)					
spectral_rssi		prev	tot	cnt	curr	prev	tot	cnt	curr	prev	tot
cnt	curr										
	1	96	8744	100	87	-95	-191	2	-95	47	79
2	39										
	6	95	9666	100	96	-121	-127747	1078	-118	30	33471
1078	31										
	11	94	9026	100	90	-96	-95	1	-95	37	47
1	47										



```
chan 6 tx_retries=0% rx_error=0% age=13 sec
```

```
*Remaining time in current period: sel 2088 Sec   Curr Chan 6 mon 287 Sec
```

```
Radio 1 Darrp yes
```

```
selection period      : 3600 sec
```

```
monitor   period      : 300 sec
```

```
weight-managed-ap     : 50
```

```
weight-rogue-ap       : 10
```

```
weight-noise-floor     : 40
```

```
weight-channel-load    : 20
```

```
weight-weather-channel : 1000
```

```
weight-dfs-channel     : 500
```

```
threshold-ap           : 250
```

```
threshold-noise-floor  : -85 dBm
```

```
threshold-channel-load : 40
```

```
threshold-spectral-rssi : -65 dBm
```

```
threshold-tx-retries   : 300%
```

```
threshold-rx-errors    : 50%
```

```
include-weather-channel : 0
```

```
include-dfs-channel    : 0
```

chan		chan_load(%)				noise_floor(dBm)					
spectral_rssi		prev	tot	cnt	curr	prev	tot	cnt	curr	prev	tot
cnt	curr										
	36	7	2051	100	20	-96	-68256	711	-96	16	11654
711	16										
	48	5	4255	100	42	-96	-192	2	-96	10	5
2	2										
	52	4	236	23	10	-96	-288	3	-96	4	21
3	7										
	56	5	277	60	4	-96	-288	3	-96	3	63
3	21										

```
chan 36 tx_retries=0% rx_error=0% age=13 sec
```

```
*Remaining time in current period: sel 2089 Sec   Curr Chan 36 mon 287 Sec
```

## Extend spectrum analysis to support FortiAPs with three radios - 6.4.2

For FortiAP models with three radios, spectrum analysis can be performed on the third radio on all channels from the 2.4 GHz and 5 GHz bands. On FortiAPs with two radios operating in AP mode, spectrum analysis can be performed on operating channels.

In the CLI, the `spectrum-analysis` property was removed from `wireless-controller wtp-profile`, and the `override-analysis` property was removed from `wireless-controller wtp`.

For more details about spectrum analysis, see [Support for spectrum analysis of FortiAP E models on page 364](#).

**Sample spectrum analysis of FAP-231E third radio:**

Diagnostics and Tools - FP231ETF20000455

FP231ETF20000455

Serial Number	FP231ETF20000455
Base MAC Address	04:d5:90:bf:4c:00
Status	Up < 24 hours
Country/Region	US
Uplink Interface	port28
IPv4 Address	10.128.100.2
Uptime	1m 36s
Version	v6.4 build0430

Actions Edit

General Health Fair

2.4 GHz Health - Radio 1 Poor

N/A

Interfering SSIDs

0

Clients

95%

Channel Utilization

5 GHz Health - Radio 2 Good

N/A

Interfering SSIDs

0

Clients

5%

Channel Utilization

Radios Clients Interfering SSIDs Logs CLI Access Spectrum Analysis VLAN Probe

Band 2.4 GHz 5 GHz

Radio Radio 3

Channels 1-13

Some or all of the channels in this range will not be scanned due to AP region.

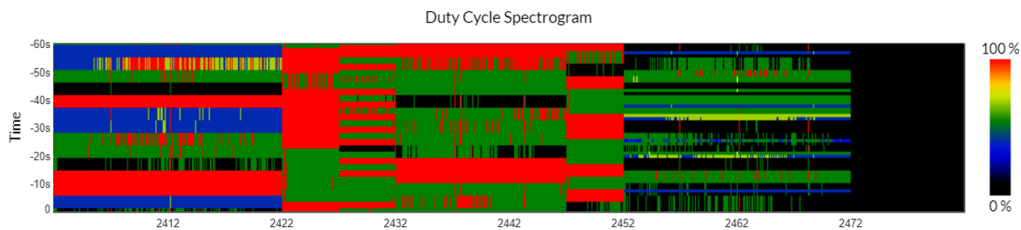
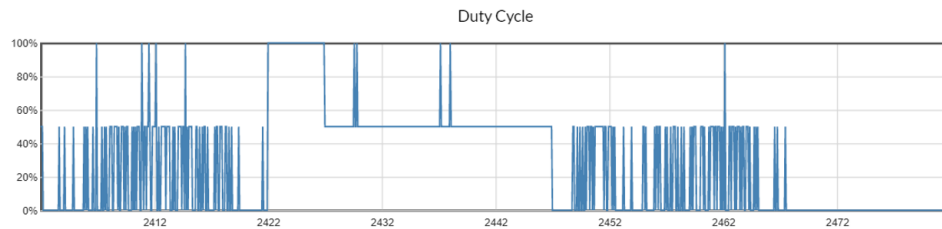
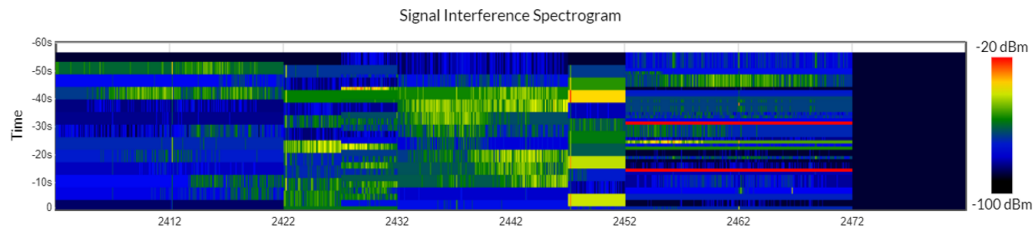
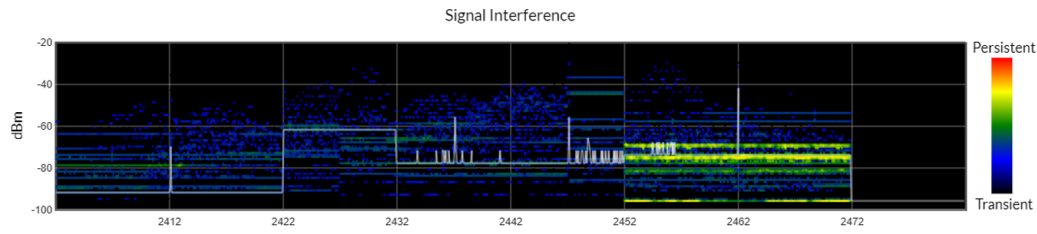
X-Axis MHz Channels

Stop Restart

Close

**Sample spectrum analysis of FAP-231E 2.4 GHz band:**

## Analysis



## Detected Interference

Type	Frequency	Last Detected
Scanning		

**Sample spectrum analysis of FAP-231E 5 GHz band:**

Band  ☒ 5 GHz

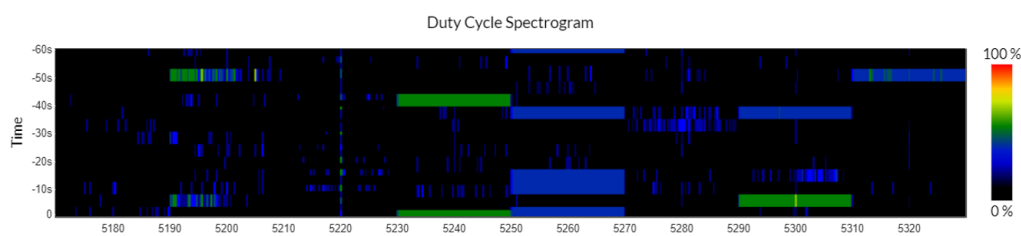
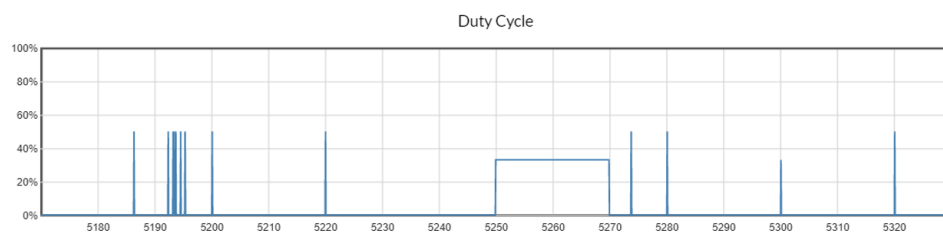
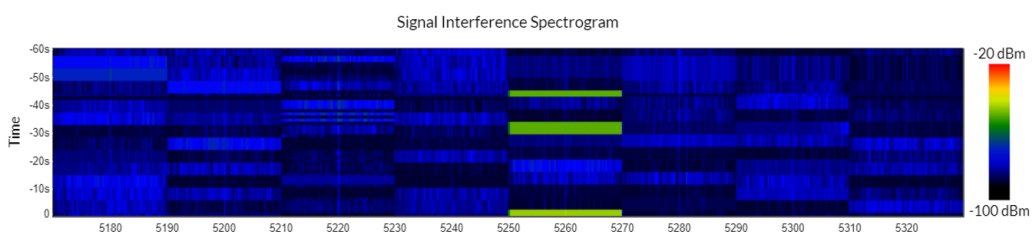
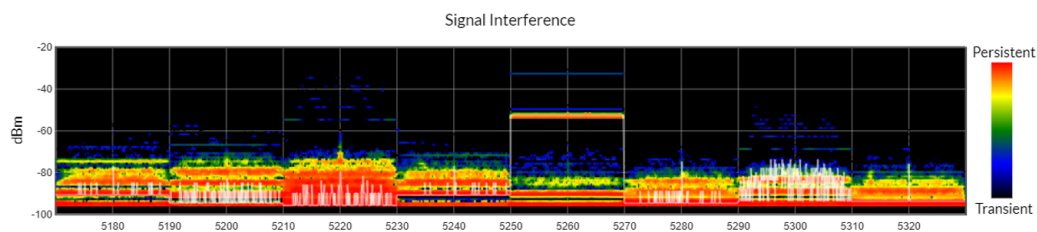
Radio ☒ Radio 3

Channels ☒ 36-64 ☐ 100-140 ☐ 149-165

X-Axis ☒ MHz ☐ Channels

☒ Stop ☐ Restart

## Analysis



## Detected Interference

Type	Frequency	Last Detected
WiFi, DSSS cordless phone	5170 MHz	2020/07/09 16:34:37

**Sample spectrum analysis of FAP-S223E with radios in AP mode:**

Click *Start* to run the spectrum analysis on the band.

Diagnostics and Tools - PS223E3X16000015

PS223E3X16000015

Serial Number PS223E3X16000015

Base MAC Address 90:6c:ac:c7:61:b8

Status Up < 24 hours

Country/Region US

Uplink Interface port26

IPv4 Address 10.100.102.100

Uptime 16h 56m 22s

Version v6.4 build0430

Actions Edit

General Health Fair

2.4 GHz Health - Radio 1 Poor

32 Interfering SSIDs

0 Clients

N/A Channel Utilization

5 GHz Health - Radio 2 Fair

7 Interfering SSIDs

0 Clients

N/A Channel Utilization

Radios

Clients

Interfering SSIDs

Logs

CLI Access

Spectrum Analysis

VLAN Probe

Band 2.4 GHz 5 GHz

Radio Radio 1

Radio 1 is operating in Access Point mode, client service may be negatively impacted during analysis.

Channels 1-13

Some or all of the channels in this range will not be scanned due to AP region.

X-Axis MHz Channels

Stop

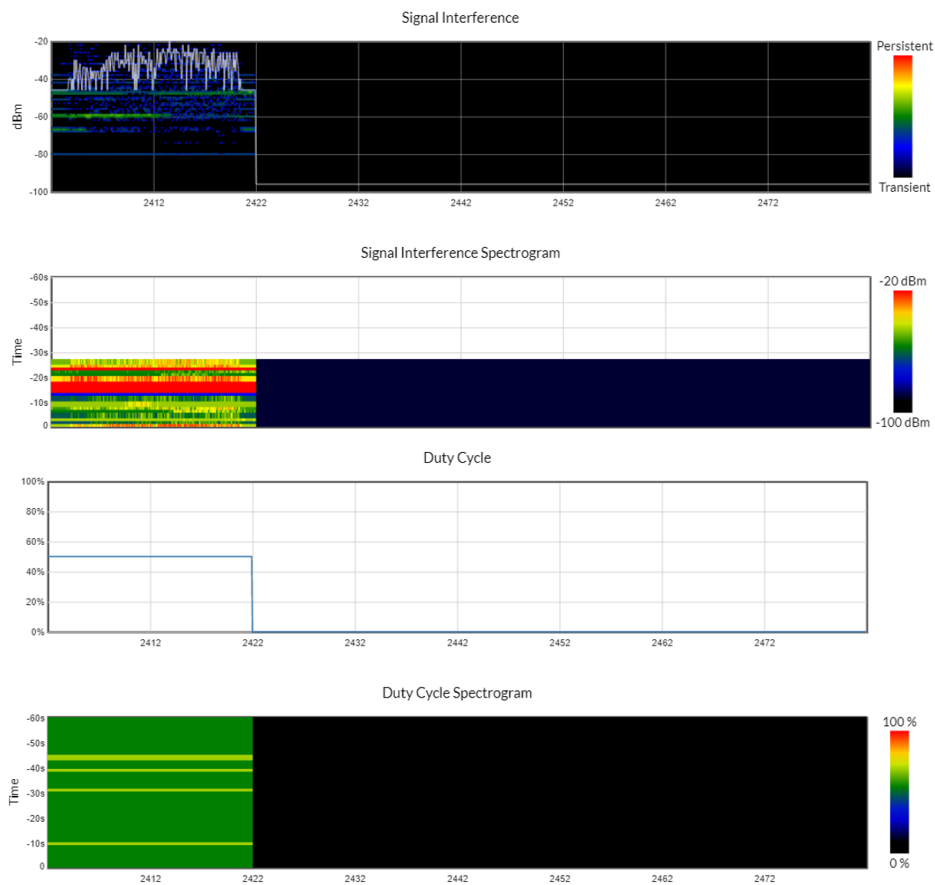
Start

- Results on operating channel of 2.4 GHz band when radio 1 is working in AP mode. In this example, the operating channel is 1.

FortiOS 6.4.0 New Features Guide  
Fortinet Inc.

407

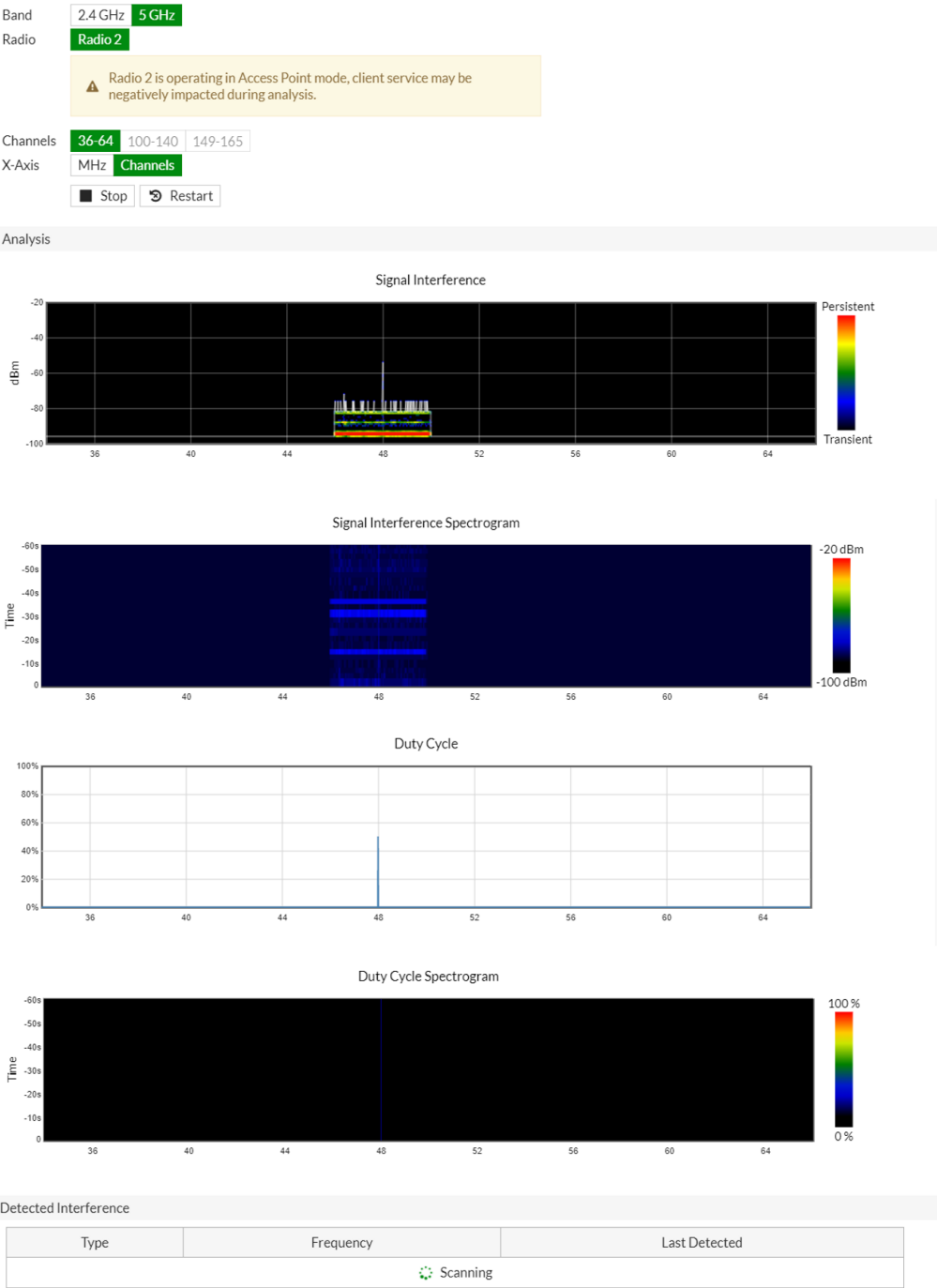
## Analysis



## Detected Interference

Type	Frequency	Last Detected
Scanning		

- Results on operating channel of 5 GHz band when radio 2 is working in AP mode. In this example, the operating channel is 48.



Antenna Rx chain status check and notification - 6.4.2

In cases where a large variance is detected in the RSSI value collected by the FortiAP, an event will be recorded in the AP diagnostics as well as in the FortiGate event logs where the antenna with the suspected failure is indicated.

**To access RSSI value reporting in FortiOS:**

```
# diagnose wireless-controller wlac -c wtp FP423E3X17000000 | grep antenna
antenna RSSI      : 42  35  29  34  (age=5)

# get wireless-controller wtp-status FP423E3X17000000 | grep antenna
antenna RSSI      : 42  35  29  34  (age=5)
```

If an external antenna is removed or a low RSSI is received from one of the AP antennas, an event is triggered and updated:

```
# diagnose wireless-controller wlac -c wtp FP423E3X17000000 | grep antenna
antenna RSSI      : 38  30  25  35  (age=10)
antenna event      : 38  30  25* 35  (age=10)
```

The WiFi event log contains a warning about the antenna failure:

```
date=2020-07-03 time=14:35:02 logid="0104043692" type="event" subtype="wireless"
level="warning" vd="root" eventtime=1593812102001404033 tz="-0700" logdesc="Defect antenna
detection" sn="FP423E3X17000357" ap="FP423E3X17000357" ip=111.168.1.2 radioid=2
radioband="802.11ac" bandwidth="20MHz" configcountry="US " opercountry="US " cfgtxpower=17
opertxpower=14 action="antenna-defect-detected" msg="AP FP423E3X17000357 radio 2 antenna
defect detected at 3.
```

**To access RSSI value reporting in FortiAP:**

```
# cw_diag -c rx-chain
Radio 0: No STAs
Radio 1:
  Chain 0: pri20  sec20  sec40  sec80
           62      0      0      0
  Chain 1: 64      0      0      0
  Chain 2: 42      0      0      0
  Chain 3: 57      0      0      0
Radio 1 prime channel RSSI history and average:
  Chain 0: 62 62 62 62 62 62 62 62 -- 62
  Chain 1: 64 64 65 64 64 64 64 64 -- 64
  Chain 2: 42 42 42 42 43 43 43 42 -- 42
  Chain 3: 56 56 57 56 57 57 57 55 -- 56
```

## Standardize wireless health metrics - 6.4.2

Health metrics calculations are standardized in the backend. Consistent colors are used to represent health status and differentiate between band frequency. The health data is now available through a REST API so that this information is standardized across other platforms.

The following colors are used for health status:

- Good = green
- Fair = yellow
- Poor = red

The following colors are used for band frequency:

- 2.4 GHz = light blue
- 5.0 GHz = dark blue



## Sample diagnostics

- **WiFi & Switch Controller > Managed FortiAPs > Diagnostics and Tools** for a select FortiAP:

Diagnostics and Tools - FP421E3X16000715

FP421E3X16000715		<b>General Health</b> <span style="color: orange;">⚠ Fair</span>
Serial Number	FP421E3X16000715	7% CPU Usage 75% Memory Usage 0 days Connection Uptime 1.0 Gbps lan1 0 Mbps lan2
Base MAC Address	90:6c:ac:e0:79:f0	<b>2.4 GHz Health - Radio 1</b> <span style="color: orange;">⚠ Fair</span>
Status	<span style="color: green;">✔</span> Up < 24 hours	5 Interfering SSIDs 1 Clients 41% Channel Utilization
Country/Region	US	<b>5 GHz Health - Radio 2</b> <span style="color: green;">✔ Good</span>
Uplink Interface	wan1	0 Interfering SSIDs 0 Clients 3% Channel Utilization
IPv4 Address	192.168.1.116	
Uptime	22h 43m 33s	
Version	v6.4 build0423	
Actions <span style="border: 1px solid black; padding: 2px;">Edit</span>		

Radios
Clients
Interfering SSIDs
Logs
CLI Access
Spectrum Analysis
VLAN Probe

	Radio 1 - 2.4 GHz	Radio 2 - 5 GHz
Mode	AP	AP
SSID	fortinet.mesh.60e (mesh) FOS_QA_Starr_60e_cap (cap) fwf-61f-psk (wifi)	fortinet.mesh.60e (mesh) FOS_QA_Starr_60E-br_cap (br2) FOS_QA_Starr_60e_cap (cap)
Clients	1	0
Bandwidth Tx	37.36 kbps	25.28 kbps

- **WiFi & Switch Controller > WiFi Clients:**

Signal Strength

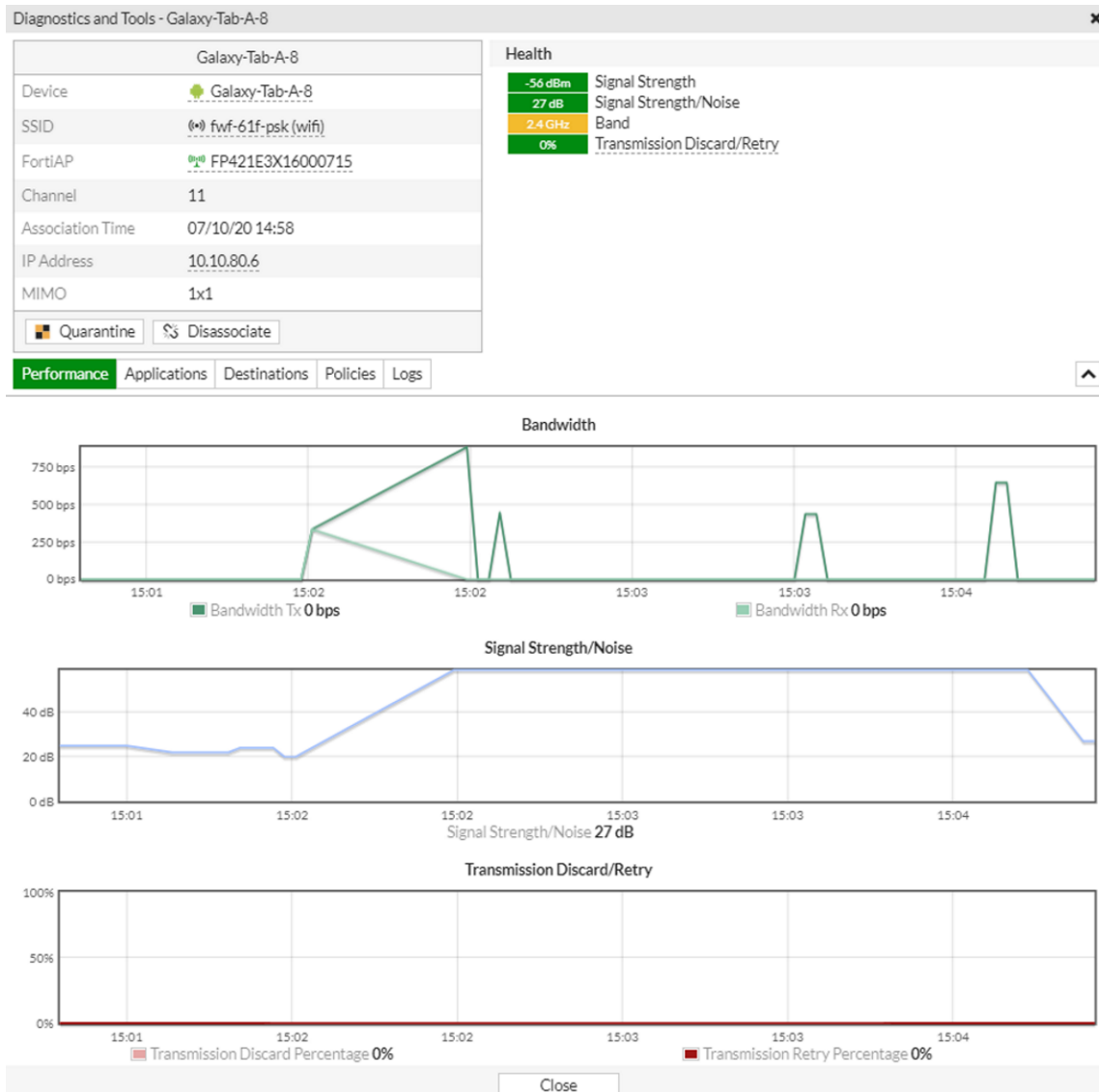
Band

Technology

Refresh
Diagnostics and Tools
Search
FortiWiFi-60E

IP	MAC Address	FortiAP	SSID	User	Device	Signal Strength	Channel	Bandwidth Tx/Rx
10.10.80.3	00:1E:E5:DF:B1:63	FP431FTF	fwf-61f-psk		我的测试wifi-win-PC	-41 dBm	36	0 bps
10.10.80.5	14:D1:69:5C:B8:DA	FP421E3X	fwf-61f-psk		HUAWEI_P20_lite	-55 dBm	11	0 bps
10.10.80.6	E0:D0:83:A7:82:11	Local WiFi Radio	fwf-61f-psk		Galaxy-Tab-A-8	-57 dBm	1	0 bps

- *WiFi & Switch Controller > WiFi Clients > Diagnostics and Tools* for a select WiFi client:



### REST API example:

`https://<FortiGate IP>/api/v2/monitor/wifi/client`

```
{
  "http_method": "GET",
  "results": [
    {
      "sta_ip": "10.10.80.6",
      "sta_ip6": [
        "::"
      ],
      "sta_rate": "52.0 mbps",
      "sta_snr": "37 dB",
      "sta_idle_time": "2 sec",
      "sta_assoc_time": "07/10/20 15:42",
    }
  ]
}
```

```
"wtp_bandwidth_Tx": "19 kbps",
"wtp_bandwidth_Rx": "6 kbps",
"wtp_bandwidth_TRx": "26 kbps",
"sta_mac": "e0:d0:83:a7:82:11",
"sta_auth": "pass",
"ip": "10.10.80.6",
"wtp_name": "FWF60E-WIFI0",
"wtp_id": "FWF60E4Q16000000",
"wtp_radio": 1,
"wtp_ip": "127.0.0.1",
"vap_name": "wifi",
"ssid": "fwf-61f-psk",
"mac": "e0:d0:83:a7:82:11",
"os": "Android",
"hostname": "Galaxy-Tab-A-8",
"authentication": "pass",
"captiver_portal_authenticated": 0,
"data_rate": 520,
"data_rate_bps": 52000000,
"snr": 37,
"idle_time": 2,
"association_time": 1594420941,
"bandwidth_tx": 6508,
"bandwidth_rx": 19774,
"lan_authenticated": false,
"channel": 1,
"signal": -58,
"vci": "",
"host": "",
"security": 10,
"encrypt": 1,
"noise": -95,
"radio_type": "802.11n",
"mimo": "1x1",
"vlan_id": 0,
"tx_discard_percentage": 0,
"tx_retry_percentage": 0,
"mpsk_name": "",
"health": {
  "signal_strength": {
    "value": -58,
    "severity": "good"
  },
  "snr": {
    "value": 37,
    "severity": "good"
  },
  "band": {
    "value": "24ghz",
```

```

"severity": "fair"
},
"transmission_retry": {
"value": 0,
"severity": "good"
},
"transmission_discard": {
"value": 0,
"severity": "good"
}
}
},
"vdom": "root",
"path": "wifi",
"name": "client",
"status": "success",
"serial": "FWF60E4Q16000000",
"version": "v6.4.0",
"build": 1705

```

## FortiAP query to FortiGuard IoT service to determine device details - 6.4.2

A FortiAP collects packets from devices and queries FortiGuard with the help of the FortiGate. Device detection results are reported back to the FortiGate where this information is displayed. Querying the FortiGuard service requires an IoT Detection Service license.

The following attributes have been added to `wireless-controller setting`:

Attribute	Description
device-weight <integer>	Set the device upper limit of confidence (0 - 255, default = 1, 0 = disable).
device-holdoff <integer>	Set the device lower limit of creation time, in minutes (0 - 60, default = 5).
device-idle <integer>	Set the device upper limit of idle time, in minutes (0 - 14400, default = 1440).

### To query the FortiGuard IoT service:

```

config wireless-controller setting
...
set device-weight 1
set device-holdoff 5
set device-idle 1440
...
end

# diagnose user device list
vd root/0 54:27:1e:e6:26:3d gen 89 req OUA/34
created 70s gen 86 seen 2s port29 gen 28
ip 10.29.1.214 src mac
hardware vendor 'Asustek compute' src fortiguard id 0 weight 21

```

```
type 'Home & Office' src fortiguard id 0 weight 21
family 'Computer' src fortiguard id 0 weight 21
os 'Linux' src dhcp id 822 weight 128
host 'test-wifi' src dhcp
```

## Enhance MPSK functionalities for wireless controller - 6.4.2

MPSK functionalities now include the ability to batch generate or import MPSK keys, export MPSK keys to a CSV file, dynamically assign VLANs based on used MPSK, and apply an MPSK schedule in the GUI.

In the GUI, MPSK key entries are organized in different MPSK groups. An MPSK group can be created manually or imported. When MPSK is enabled, the previous single passphrase is dropped and a dynamic VLAN is automatically enabled.

In the CLI, an `mpsk-profile` is assigned in the VAP settings and MPSK is enabled. The dynamic VLAN is automatically enabled. Only one MPSK profile can be assigned to one VAP at a time.

### To use an MPSK group in the GUI:

1. Go to *WiFi & Switch Controller > SSIDs* and click *Create New > SSID*.
2. Enter a name and ensure the *Security mode* is set to *WPA2 Personal*.
3. In the *Pre-shared Key* section, select a *Mode* (*Multiple* is used in this example).
4. In the table, click *Add > Create Group*.

The screenshot shows the 'Edit Interface' configuration for a WiFi-mpsk (wifi-mpsk) SSID. The 'Pre-shared Key' section is expanded, showing a table with columns for Name, VLAN ID, and Keys. The 'Mode' is set to 'Multiple'. The table contains two rows: 'group-a' with VLAN ID 10 and Keys 1, and 'group-b' with VLAN ID 20 and Keys 1. The 'Add' button is highlighted, and the 'Create Group' option is selected in the dropdown menu.

Name	VLAN ID	Keys
group-a	10	1
group-b	20	1

5. Enter a group name and VLAN ID.

## 6. Configure the pre-shared key settings:

### a. In the table, click *Add > Generate Keys*.

The screenshot shows the 'Edit Interface' window on the left and the 'Edit Multiple Pre-shared Key Group' dialog on the right.

**Edit Interface (Left):**

- Name: FOS-QA-LFU-mpsk (wifi-mpsk)
- Alias: b
- Type: WIFI SSID
- Traffic mode: Bridge
- WIFI Settings:
  - SSID: FOS-QA-LFU-mpsk
  - Client limit: ☐
  - Broadcast SSID: ☒
- Security Mode Settings:
  - Security mode: WPA2 Personal
- Pre-shared Key:
  - Mode: Multiple
  - Table:
 

Group Name	VLAN ID	Keys
group-a	10	1
group-b	20	1
- Client MAC Address Filtering:
  - RADIUS server: ☐
- Additional Settings:
  - Local standalone: ☐
  - Local authentication: ☐
  - Schedule: always

**Edit Multiple Pre-shared Key Group (Right):**

- Group name: group-a
- VLAN ID: 10 (1 - 4094)
- Pre-shared Keys:
 

MAC Address	Client Limit	Schedule	Comments
Not assigned	Default	always	
- Buttons: OK, Cancel

### b. Configure the settings as needed and click *OK*.

The screenshot shows the 'Edit Interface' window on the left and the 'Generate Keys' dialog on the right.

**Edit Interface (Left):**

- Name: wifi-mpsk (wifi-mpsk)
- Alias: b
- Type: WIFI SSID
- Traffic mode: Bridge
- WIFI Settings:
  - SSID: wifi-mpsk
  - Client limit: ☐
  - Broadcast SSID: ☒
- Security Mode Settings:
  - Security mode: WPA2 Personal
- Pre-shared Key:
  - Mode: Multiple
  - Table:
 

Group Name	VLAN ID	Keys
group-a	10	1
group-b	20	1
- Client MAC Address Filtering:
  - RADIUS server: ☐
- Additional Settings:
  - Local standalone: ☐
  - Local authentication: ☐
  - Schedule: always

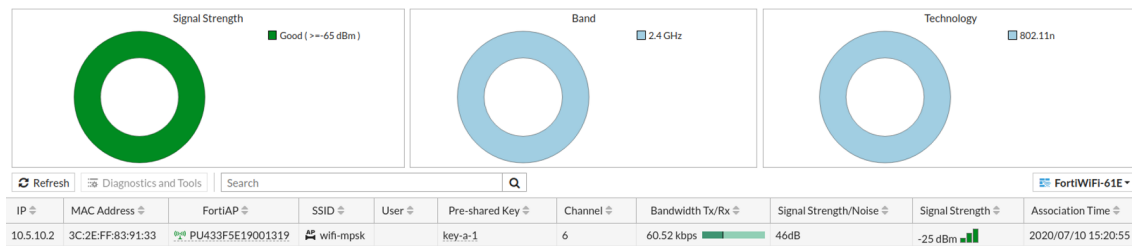
**Generate Keys (Right):**

- Name prefix: autugen
- Number of keys: 100 (1 - 15998)
- Key length: 10 (8 - 63)
- Client limit: Default Unlimited Specify
- Schedule: always
- Buttons: OK, Cancel

## 7. Click *OK* to close the *Pre-shared Key Group* window.

## 8. Click *OK*.

9. Go to *WiFi & Switch Controller > WiFi Clients* to view the MPSK name in the *Pre-shared Key* column.



## To use an MPSK profile in the CLI:

1. Configure the MPSK profile:

```
config wireless-controller mpsk-profile
  edit "wifi-mpsk"
    config mpsk-group
      edit "group-a"
        set vlan-type fixed-vlan
        set vlan-id 10
        config mpsk-key
          edit "key-a-1"
            set passphrase ENC
            set mpsk-schedules "always"
          next
        end
      next
    edit "group-b"
      set vlan-type fixed-vlan
      set vlan-id 20
      config mpsk-key
        edit "key-b-1"
          set passphrase ENC
          set concurrent-client-limit-type unlimited
          set mpsk-schedules "always"
        next
      end
    next
  end
end
next
end
```

2. Configure the VAP settings:

```
config wireless-controller vap
  edit "wifi-mpsk"
    set ssid "wifi-mpsk"
    set local-bridging enable
    set schedule "always"
    set mpsk-profile "wifi-mpsk"
    set dynamic-vlan enable
  next
end
```

**3. Verify the event log after the WiFi client is connected:**

```
1: date=2020-07-10 time=16:57:20 logid="0104043573" type="event" subtype="wireless"
level="notice" vd="root" eventtime=1594425440439070726 tz="-0700" logdesc="Wireless
client authenticated" sn="FP423E3X16000320" ap="FP423E3X16000320" vap="wifi-mpsk"
ssid="wifi-mpsk" radioid=2 user="N/A" group="N/A" stamac="3c:2e:ff:83:91:33"
srcip=10.0.10.2 channel=144 radioband="802.11ac" signal=-52 snr=50 security="WPA2
Personal" encryption="AES" action="client-authentication" reason="Reserved 0" mpsk="key-
a-1" msg="Client 3c:2e:ff:83:91:33 authenticated."
```

**Adaptive radio architecture support - 6.4.3**

Adaptive Radio Architecture (ARA) centralizes and improves the overall efficiency of the wireless network. Dynamic Radio Mode Assignment (DRMA) is a feature in ARA that enables FortiAPs to calculate the network coverage factor (NCF) based on radio interference.

When DRMA is enabled in the WTP profile or on the specific AP, the APs run in automatic mode. The AC assigns the radio mode to the APs based on the DRMA NCF value that is calculated at each configured interval.

The NCF value is calculated based on overlapping coverage in a radio coverage area. If a radio is determined to be redundant based on the configured NCF threshold, then it switches from AP mode to monitor mode. When the NCF is next calculated, if the value is below the threshold then the radio switches back to AP mode.

**To configure the DRMA interval:**

```
config wireless-controller timers
    set drma-interval <integer>
end
```

Where:

drma-interval	Dynamic radio mode assignment (DRMA) schedule interval, in minutes (1 - 1440, default = 60).
---------------	--

**To configure DRMA on a specific AP device:**

```
config wireless-controller wtp
    edit <id>
        config <radio>
            set drma-manual-mode {ap | monitor | ncf | ncf-peek}
        end
    next
end
```

The manual mode options include:

ap	Set the radio to AP mode.
monitor	Set the radio to monitor mode
ncf	Select and set the radio mode based on the NCF score (default).
ncf-peek	Select the radio mode based on the NCF score, but do not apply it.



**To configure DRMA in a WTP profile:**

```
config wireless-controller wtp-profile
  edit <profile>
    config <radio>
      set drma enable
      set drma-sensitivity {low | medium | high}
    end
  next
end
```

DRMA is disabled by default. The sensitivity options are:

low	Consider a radio as redundant when its NCF is 100% (default).
medium	Consider a radio as redundant when its NCF is 95%.
high	Consider a radio as redundant when its NCF is 90%.

**Diagnose commands****To display the calculated DRMA results:**

```
# diagnose wireless-controller wlac -c wtp-drma-radio 1
```

**To manually start the DRMA evaluation:**

```
# diagnose wireless-controller wlac -c wtp-drma-eval
```

**To manually change the WTP radio mode:**

```
# diagnose wireless-controller wlac -c wtp-drma-mode wtp-id rId {ap | monitor | ncf}
# diagnose wireless-controller wlac -c ws-drma-mode vfid-ip:port rId {ap | monitor | ncf}
```

These commands immediately change the WTP or WS radio operating DRMA mode.

**To enable the DRMA related daemon log:**

```
# diagnose wireless-controller wlac debug drma 5
# diagnose debug enable
```

**Example**

In this example, DRMA is enabled in the WTP profile and the sensitivity is set to high. A FortiAP using the profile is put into monitor mode when NCF drops below the threshold, and then goes back into AP mode when the NCF goes back above the threshold.

**To configure the WTP profile and apply it to the AP:**

```
config wireless-controller wtp-profile
  edit "FAP423E-default"
    config platform
```

```

        set type 423E
    end
    set wan-port-mode wan-lan
    set handoff-sta-thresh 55
    set ap-country US
    set allowaccess https ssh snmp
    set login-passwd-change yes
    set login-passwd *****
    config radio-1
        set band 802.11n,g-only
        set drma enable
        set drma-sensitivity high
    end
    config radio-2
        set band 802.11ac
    end
    config lbs
        set station-locate enable
    end
next
end

config wireless-controller wtp
    edit "FP423E3X17000357"
        set admin enable
        set region "s"
        set region-x "0.5617862681516"
        set region-y "0.2023121387283"
        set wtp-profile "FAP423E-default"
        config radio-1
            end
        config radio-2
            end
    next
end

```

## Results

When the interference is too high, the AP is put into monitor mode. When the interference goes back below the threshold, the AP is put back into AP mode.

### To view the results when the AP is put into monitor mode:

```

# diagnose wireless-controller wlac -c wtp-drma-radio 1

41652.277 cwTimerDrmaIntervalHandler,739 begin
41652.277 cwAcWsDrmaHndl,689 ws (0-15.5.5.1:5246):0 re 0x657f8c0 ddscan_re (nil)
41652.277 cwAcWsDrmaRadioNcf,519 band_5g 0 wr PU421ETF19005587,0 chan 11 noise -95 snr 10
...
41652.279 cwAcWsDrmaRadioNcf,567 band_5g 0 re FP423E3X17000357,0 drma_wr_cnt 4 tot ncf 350
41652.279 cwAcWsDrmaHndl,700 ws (0-15.5.5.1:5246):0 wr_n 0 drma 1 mmode(ncf) ncf 94 thresh
90 monitor 0(0) ==> ncf eval 1
41652.279 cwAcWsRadioModeSet,647 ws (0-15.5.5.1:5246):0 curr oper mode 0 new mode 1
41652.280 cwAcSendCfgUpdReq_vap_downup,4310 ws (0-15.5.5.1:5246) rId 0 wId 0 downup 1
41652.280 cwAcWsVapModeMark ws (0-15.5.5.1:5246):0,0 mon 1 ws (0-6.6.6.2:5246):2 wr
FP423E3X17000357,0 !

```

```
...
41652.283 cwTimerDrmaIntervalHandler,747 end
```

The results show that the NCF is 94%, which is above the threshold of 90%, so the AP mode is changed to monitor.

The following logs are generated, showing that the AP is now in monitor mode:

```
date=2020-08-19 time=11:04:20 logid="0104043697" type="event" subtype="wireless"
level="notice" vd="root" eventtime=1597860260283044465 tz="-0700" logdesc="Physical AP radio
DRMA stop" sn="FP423E3X17000357" ap="FP423E3X17000357" ip=15.5.5.1 radioid=1
radioband="802.11n,g-only" bandwidth="20MHz" configcountry="US " opercountry="US "
cfgtxpower=27 opertxpower=3 slctdrmamode="monitor" operdrmamode="monitor" action="drma-stop"
msg="AP FP423E3X17000357 radio 1 DRMA stopped."
```

```
date=2020-08-19 time=11:04:20 logid="0104043698" type="event" subtype="wireless"
level="notice" vd="root" eventtime=1597860260282952255 tz="-0700" logdesc="Physical AP radio
DRMA mode" sn="FP423E3X17000357" ap="FP423E3X17000357" ip=15.5.5.1 radioid=1
radioband="802.11n,g-only" bandwidth="20MHz" configcountry="US " opercountry="US "
cfgtxpower=27 opertxpower=3 slctdrmamode="monitor" operdrmamode="monitor" action="drma-mode"
msg="AP FP423E3X17000357 radio 1 DRMA selected mode monitor operating mode monitor."
```

```
date=2020-08-19 time=11:04:20 logid="0104043696" type="event" subtype="wireless"
level="notice" vd="root" eventtime=1597860260277325993 tz="-0700" logdesc="Physical AP radio
DRMA start" sn="FP423E3X17000357" ap="FP423E3X17000357" ip=15.5.5.1 radioid=1
radioband="802.11n,g-only" bandwidth="20MHz" configcountry="US " opercountry="US "
cfgtxpower=27 opertxpower=3 slctdrmamode="ap" operdrmamode="ap" action="drma-start" msg="AP
FP423E3X17000357 radio 1 DRMA started."
```

To view the results when the AP goes back into AP mode:

```
# diagnose wireless-controller wlac -c wtp-drma-radio 1
```

```
41712.277 cwTimerDrmaIntervalHandler,739 begin
41712.277 cwAcWsDrmaHndl,689 ws (0-15.5.5.1:5246):0 re 0x657f8c0 ddscan_re (nil)
41712.277 cwAcWsDrmaRadioNcf,519 band_5g 0 wr PU421ETF19005587,0 chan 1 noise -95 snr 11
...
41712.279 cwAcWsDrmaRadioNcf,567 band_5g 0 re FP423E3X17000357,0 drma_wr_cnt 4 tot ncf 344
41712.279 cwAcWsDrmaHndl,700 ws (0-15.5.5.1:5246):0 wr_n 0 drma 1 mmode(ncf) ncf 88 thresh
90 monitor 1(1) ==> ncf eval 0
41712.279 cwAcWsRadioModeSet,647 ws (0-15.5.5.1:5246):0 curr oper mode 1 new mode 0
41712.279 cwAcSendCfgUpdReq_vap_downup,4310 ws (0-15.5.5.1:5246) rId 0 wId 0 downup 0
41712.280 cwAcWsVapModeMark ws (0-15.5.5.1:5246):0,0 mon 0 ws (0-6.6.6.2:5246):2 wr
FP423E3X17000357,0 !
...
41712.282 cwTimerDrmaIntervalHandler,747 end
```

The results show that the NCF is now 88%, which is above the threshold of 90%, so the mode is changed back to AP.

The following logs are generated:

```
date=2020-08-19 time=11:05:20 logid="0104043697" type="event" subtype="wireless"
level="notice" vd="root" eventtime=1597860320282294450 tz="-0700" logdesc="Physical AP radio
DRMA stop" sn="FP423E3X17000357" ap="FP423E3X17000357" ip=15.5.5.1 radioid=1
radioband="802.11n,g-only" bandwidth="20MHz" configcountry="US " opercountry="US "
cfgtxpower=27 opertxpower=3 slctdrmamode="ap" operdrmamode="ap" action="drma-stop" msg="AP
FP423E3X17000357 radio 1 DRMA stopped."
```

```
date=2020-08-19 time=11:05:20 logid="0104043698" type="event" subtype="wireless"
```

```
level="notice" vd="root" eventtime=1597860320282202827 tz="-0700" logdesc="Physical AP radio
DRMA mode" sn="FP423E3X17000357" ap="FP423E3X17000357" ip=15.5.5.1 radioid=1
radioband="802.11n,g-only" bandwidth="20MHz" configcountry="US " opercountry="US "
cftgtxpower=27 opertxpower=3 slctdrmamode="ap" operdrmamode="ap" action="drma-mode" msg="AP
FP423E3X17000357 radio 1 DRMA selected mode ap operating mode ap."
```

```
date=2020-08-19 time=11:05:20 logid="0104043696" type="event" subtype="wireless"
level="notice" vd="root" eventtime=1597860320277336047 tz="-0700" logdesc="Physical AP radio
DRMA start" sn="FP423E3X17000357" ap="FP423E3X17000357" ip=15.5.5.1 radioid=1
radioband="802.11n,g-only" bandwidth="20MHz" configcountry="US " opercountry="US "
cftgtxpower=27 opertxpower=3 slctdrmamode="monitor" operdrmamode="monitor" action="drma-
start" msg="AP FP423E3X17000357 radio 1 DRMA started."
```

## Support 802.11v optimized roaming and load balancing - 6.4.3

When a FortiGate detects the client RSSI is outside of the threshold, the FortiAP sends a BSTM (802.11v BSS transition management) request to the client. The client can either accept the request because the FortiAP can provide a strong RSSI, or reject the request because the RSSI from the FortiAP is very weak.

When voice-enterprise is enabled, sticky-client-remove is automatically enabled. Use sticky-client-threshold-5g to edit the minimum signal level.

### Disassociation function

If a client is capable of BSS transition, the AP sends the client a BSTM request instead of disassociating with the client.

In this configuration, the client connects to the FortiAP within the threshold range:

```
config wireless-controller vap
    edit "81e ssid11v"
        set ssid "test_11v"
        set voice-enterprise enable
        set sticky-client-remove enable
        set sticky-client-threshold-5g "-45"
    next
end

# diagnose wireless-controller wlac -d sta
vf=2 wtp=3 rId=2 wlan=81e ssid11v vlan_id=0 ip=10.11.123.2 ip6=fe80::146b:d5f8:fd2d:fb0e
mac=d4:a3:3d:01:62:4f vci= host=WiFi-QA-iPhone8 user= group= signal=-34 noise=-95 idle=0
bw=677 use=6 chan=153 radio_type=11AC security=wpa2_only_personal mpsk= encrypt=aes cp_
authed=no online=yes mimo=2
```

If the threshold is changed to request a strong signal that is outside of the threshold, the AP sends a request and receives a reject response from the client:

```
config wireless-controller vap
    edit "81e ssid11v"
        set ssid "test_11v"
        set voice-enterprise enable
        set sticky-client-remove enable
        set sticky-client-threshold-5g "-20"
    next
end
```

The WiFi event log contains the BSTM reject response:

```

3: date=2020-09-18 time=16:08:37 logid="0104043695" type="event" subtype="wireless"
level="notice" vd="vdom1" eventtime=1600470517188697388 tz="-0700" logdesc="Wireless client
sent WNM action BSTM response reject" sn="FP421ETF19003703" ap="FP421ETF19003703" vap="81e_
ssid11v" ssid="test_11v" radioid=2 user="N/A" stamac="d4:a3:3d:01:62:4f" channel=48
security="WPA2 Personal" encryption="AES" action="WNM-action-bstm-resp-reject"
reason="Reserved 0" msg="AP received WNM action BSTM response frame (reject) from client
d4:a3:3d:01:62:4f" remotewtptime="2949.236951"

4: date=2020-09-18 time=16:08:37 logid="0104043693" type="event" subtype="wireless"
level="notice" vd="vdom1" eventtime=1600470517188517242 tz="-0700" logdesc="AP sent WNM
action BSTM request" sn="FP421ETF19003703" ap="FP421ETF19003703" vap="81e_ssid11v"
ssid="test_11v" radioid=2 user="N/A" stamac="d4:a3:3d:01:62:4f" channel=48 security="WPA2
Personal" encryption="AES" action="WNM-action-bstm-req" reason="Reserved 0" msg="AP sent WNM
action BSTM request frame to client d4:a3:3d:01:62:4f" remotewtptime="2949.235888"

```

## Association RSSI check

If a client is capable of BSS transition, the client is allowed to associate and the AP sends the client a BSTM request.

In this configuration, the client is able to connect to the SSID outside of the range. The AP sends the BSTM request to the client, and the client will decide whether or not to associate.

```

config wireless-controller vap
    edit "81e_ssid11v"
        set ssid "test_11v"
        set voice-enterprise enable
        set sticky-client-remove enable
        set sticky-client-threshold-5g "-45"
    next
end

# diagnose wireless-controller wlaac -d sta
vf=2 wtp=3 rId=2 wlan=81e_ssid11v vlan_id=0 ip=10.11.123.2 ip6=fe80::146b:d5f8:fd2d:fb0e
mac=d4:a3:3d:01:62:4f vci= host=WiFi-QA-iPhone8 user= group= signal=-54 noise=-95 idle=3
bw=5 use=6 chan=153 radio_type=11AC security=wpa2_only_personal mpsk= encrypt=aes cp_
authed=no online=yes mimo=2

```

The WiFi event log contains the BSTM request:

```

3: date=2020-09-18 time=15:52:44 logid="0104043693" type="event" subtype="wireless"
level="notice" vd="vdom1" eventtime=1600469564377293204 tz="-0700" logdesc="AP sent WNM
action BSTM request" sn="PS223E3X17000006" ap="PS223E3X17000006" vap="81e_ssid11v"
ssid="test_11v" radioid=2 user="N/A" stamac="d4:a3:3d:01:62:4f" channel=153 security="WPA2
Personal" encryption="AES" action="WNM-action-bstm-req" reason="Reserved 0" msg="AP sent WNM
action BSTM request frame to client d4:a3:3d:01:62:4f" remotewtptime="1995.307607"

```

## Load balancing

If a client is rejected when load balancing fails, the client might be unsure of which AP to associate to and could repeatedly retry the same AP. If a client is capable of BSS transition, it will not try the loaded AP. The client will join by choosing an AP from the provided list.

In this example, two FortiAPs broadcast to the 81e\_ssid11v SSID. The client is able to connect with FAP-1 first. If the RSSI signal of FAP-1 is reduced, a BSTM request is sent to FAP-2. Then, FAP-2 accepts the request and the client moves to FAP-2.

**To configure load balancing:****1. Configure the VAP:**

```
config wireless-controller vap
    edit "81e_ssid11v"
        set ssid "test_11v"
        set voice-enterprise enable
        set sticky-client-remove enable
        set sticky-client-threshold-5g "-45"
    next
end
```

**2. Verify access control:**

```
# diagnose wireless-controller wlac -d sta

vf=2 wtp=2 rId=2 wlan=81e_ssid11v vlan_id=0 ip=10.11.123.2 ip6=fe80::146b:d5f8:fd2d:fb0e
mac=d4:a3:3d:01:62:4f vci= host=WiFi-QA-iPhone8 user= group= signal=-44 noise=-95 idle=8
bw=0 use=6 chan=48 radio_type=11AC security=wpa2_only_personal mpsk= encrypt=aes cp_
authed=no online=yes mimo=2
```

**3. Verify the WiFi event log:**

```
11: date=2020-09-18 time=15:23:43 logid="0104043693" type="event" subtype="wireless"
level="notice" vd="vdom1" eventtime=1600467823308451794 tz="-0700" logdesc="AP sent WNM
action BSTM request" sn="PS223E3X17000006" ap="PS223E3X17000006" vap="81e_ssid11v"
ssid="test_11v" radioid=2 user="N/A" stamac="d4:a3:3d:01:62:4f" channel=153
security="WPA2 Personal" encryption="AES" action="WNM-action-bstm-req" reason="Reserved
0" msg="AP sent WNM action BSTM request frame to client d4:a3:3d:01:62:4f"
remotewtptime="254.178245"

12: date=2020-09-18 time=15:23:43 logid="0104043694" type="event" subtype="wireless"
level="notice" vd="vdom1" eventtime=1600467823146171299 tz="-0700" logdesc="Wireless
client sent WNM action BSTM response accept" sn="FP421ETF19003703" ap="FP421ETF19003703"
vap="81e_ssid11v" ssid="test_11v" radioid=2 user="N/A" stamac="d4:a3:3d:01:62:4f"
channel=48 security="WPA2 Personal" encryption="AES" action="WNM-action-bstm-resp-
accept" reason="Reserved 0" msg="AP received WNM action BSTM response frame (accept)
from client d4:a3:3d:01:62:4f" remotewtptime="255.413432"
```

**Support IGMP Snooping (Wireless) - 6.4.3**

Enabling IGMP snooping on a SSID allows the wireless controller to detect which FortiAP(s) have IGMP clients. The wireless controller will only forward a multicast stream to the FortiAP where there is a listener for the multicast group.

IGMP snooping on SSID can prevent WiFi clients/hosts from receiving traffic for a multicast group they have not explicitly joined. Upon detecting clients' multicast group IDs, FortiAPs join the corresponding multicast groups and the controller sends multicast packets to only CAPWAP multicast groups. Thus, the controller can prune multicast traffic from managed FortiAPs that do not contain a multicast listener (an IGMP client).

FortiGate and FortiWiFi have managed some FortiAP units that are broadcasting the same SSID with IGMP snooping enabled. Some multicast clients and non-multicast clients have been associated with the SSID.

**To enable or disable IGMP snooping in the CLI:**

```
config wireless-controller vap
    edit "test"
```

```

        set igmp-snooping {enable | disable}
    next
end

```

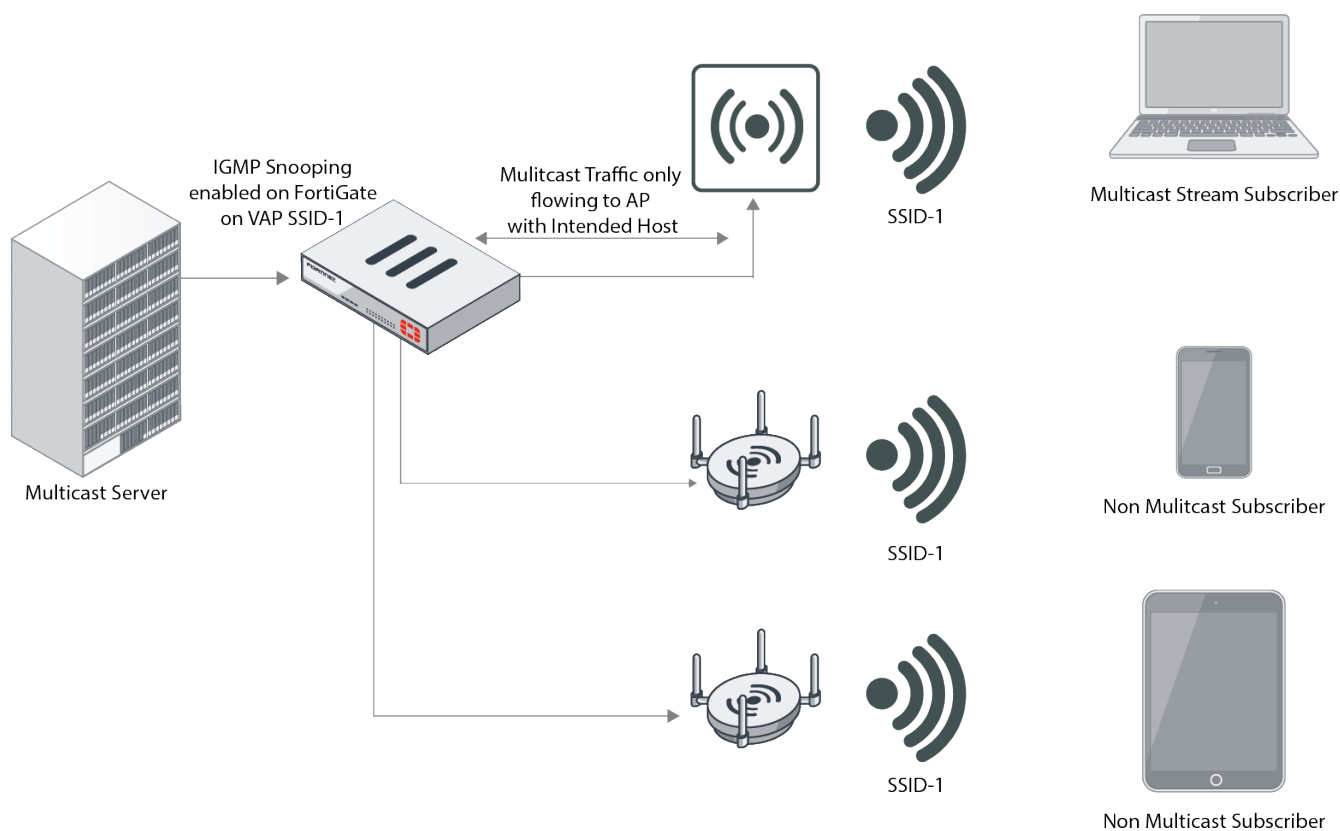
### To debug IGMP snooping:

```
diagnose wireless-controller wlac -c vap-mcgrp
```

### Example

In the example below, the VAP named `smart_test` (igmp snooping enabled) is applied to two FortiAPs, `FAP U-223` and `FAP-423E` respectively. In our test scenario we have Multicast Server on the wired side and multicast hosts are connected to VAP `smart_test`, beaoning from `FAP 423E`.

Note that there are no multicast clients for `smart_test` connected to `FAPU223E`. The multicast stream address used in the test is `235.1.1.1`, other addresses which appear in the multicast table output are well-know multicast addresses.



### To view hosts receiving the multicast traffic in the CLI:

#### 1. Debug IGMP snooping:

```

# diagnose wireless-controller wlac -c ws
-----WTP SESSION 1-----
WTP session           : 0-39.1.1.2:5246  CWAS_RUN
Ctrl in_ifIdx         : 14/port6
indev                  : 14/port6
Data in_ifIdx         : 14/port6

```

```

indev          : 0/
mesh uplink    : ethernet
id             : PU223ETF18003869
mgmt_vlanid    : 0
wtp_wanlan_mode : wan-only
refcnt         : 9
deleted        : no
plain_ctl      : disabled
wtp-mode       : normal
wtp-report-index : 2
data-chan-sec  : clear-text
ctl-msg-offload : ac=01ff/wtp_loc=01ff/wtp_rem=01ff/oper=01ff
session_id     : 19aa6b160c33edae329053a0259fd02b
ehapd cfg      : done
message queue  : 0/128 max 100
tId_10_sec     : 177810
Ekahau         : disabled
Aeroscout      : disabled
FortiPresence  : disabled
Radio 1        : AP
wlan cfg       : smart_test
vap-01(1)      : smart_test      00:0c:e6:6e:dd:65    lsw      smart_test
  Config success State RUN
Radio 2        : AP
wlan cfg       : smart_test
vap-01(1)      : smart_test      00:0c:e6:6e:dd:71    lsw      smart_test
  Config success State RUN
Radio 3        : Not Exist
Radio 4        : Not Exist
Radio 5        : Not Exist
-----WTP SESSION      2-----
WTP session    : 0-15.5.5.1:5246    CWAS_RUN
Ctrl in_ifIdx  : 97/vlan55
indev          : 97/vlan55
Data in_ifIdx  : 97/vlan55
indev          : 0/
mesh uplink    : ethernet
id             : FP423E3X17000357
mgmt_vlanid    : 55
wtp_wanlan_mode : wan-only
refcnt         : 9
deleted        : no
plain_ctl      : disabled
wtp-mode       : normal
wtp-report-index : 6
data-chan-sec  : clear-text
ctl-msg-offload : ac=01ff/wtp_loc=01ff/wtp_rem=01ff/oper=01ff
session_id     : 1425837710fd85f132fc718424a514f0
ehapd cfg      : done
message queue  : 0/128 max 18
tId_10_sec     : 177811
Ekahau         : disabled
Aeroscout      : disabled
FortiPresence  : disabled
Radio 1        : AP
wlan cfg       : smart_test

```



```

vap-01(1)      : smart_test      90:6c:ac:fa:9a:38   lsw      smart_test
  Config success State RUN
Radio 2        : AP
wlan cfg       : smart_test
vap-01(1)      : smart_test      90:6c:ac:fa:9a:40   lsw      smart_test
  Config success State RUN
Radio 3        : Virtual Lan AP
wlan cfg       :
Radio 4        : Not Exist
Radio 5        : Not Exist

```

- 2. When the hosts join the multicast group through FAP-423E, Fortigate registers the intended hosts for multicasts as shown by the CLI debug below:**

```

90672.765 cwAcUpd_vsp_mcgrp_event: mcast group report from FP423E3X17000357 radio 0 wlan
0.
90672.765 cwAc_mcgrp_sta_add6: sta 50:1a:c5:e9:0b:b3 add ff02::1:ff53:c177
90672.766 cwAc_mcgrp_vap_add6: wtp FP423E3X17000357 radio 0 wlan 0 bssid
90:6c:ac:fa:9a:38 add ff02::1:ff53:c177
90673.449 cwAcUpd_vsp_mcgrp_event: mcast group report from FP423E3X17000357 radio 0 wlan
0.
90673.449 cwAc_mcgrp_sta_add4: sta 50:1a:c5:e9:0b:b3 add 224.0.0.252
90673.449 cwAc_mcgrp_vap_add4: wtp FP423E3X17000357 radio 0 wlan 0 bssid
90:6c:ac:fa:9a:38 add 224.0.0.252
90673.450 cwAcUpd_vsp_mcgrp_event: mcast group report from FP423E3X17000357 radio 0 wlan
0.

```

- 3. The FortiAP output shows in detail the hosts that are receiving the multicast traffic.**

```

FortiAP-423E # cw_diag -c mcgrp
Interface wlan00:
  IPv4 mcast group: total 2
    224.0.0.252
    239.255.255.250
  STA 50:1a:c5:e9:0b:b3 mcast group: total 2
    224.0.0.252
    239.255.255.250
  IPv6 mcast group: total 1
    ff02::1:ff53:c177
  STA 50:1a:c5:e9:0b:b3 mcast group: total 1
    ff02::1:ff53:c177
Interface wlan10:
  IPv4 mcast group: total 4
    235.1.1.1
    239.255.255.250
    235.80.68.83
    239.83.100.109
  STA 58:00:e3:98:d1:c7 mcast group: total 3
    239.255.255.250
    235.80.68.83
    239.83.100.109
  STA d4:53:83:79:28:66 mcast group: total 1
    235.1.1.1
  IPv6 mcast group: total 3
    ff02::1:ff79:2866
    ff02::1:ff84:e0f6
    ff02::1:ff7d:1760

```

```

STA 58:00:e3:98:d1:c7 mcast group: total 1
ff02::1:ff84:e0f6
STA 68:e7:c2:df:2f:df mcast group: total 1
ff02::1:ff7d:1760
STA d4:53:83:79:28:66 mcast group: total 1
ff02::1:ff79:2866

```

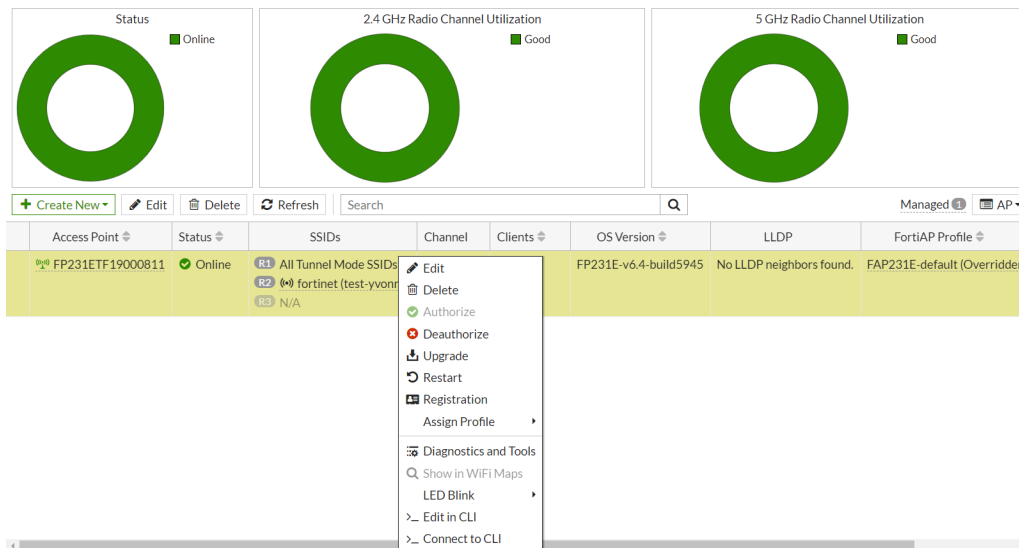
## Use FortiGate to register managed FortiAP to FortiCloud - 6.4.3

After authorizing a FortiAP, the administrator can register the FortiAP to FortiCloud directly from the FortiGate GUI.

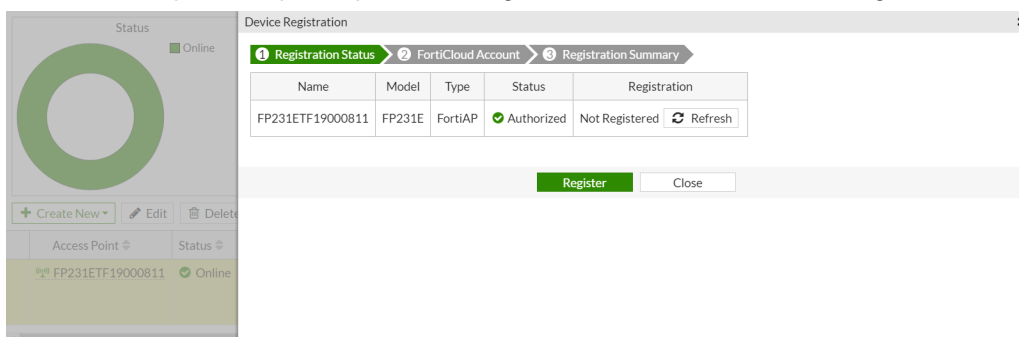
The FortiAP registration status can be viewed on the *Diagnostics and Tools* page.

**To register a FortiAP to FortiCloud when the FortiAP is authorized and online:**

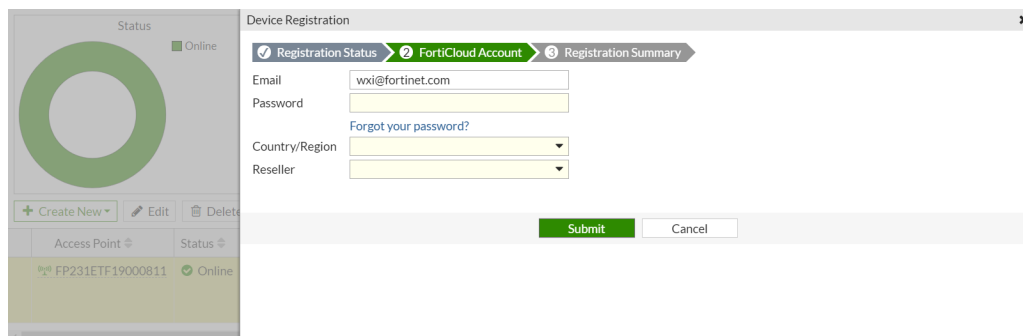
1. Go to *WiFi & Switch Controller > Managed FortiAPs* and right click on the FortiAP.



2. Click *Registration*. This option is not available if the device is detected but not authorized. The *Device Registration* pane opens, showing the device information and its registration status.



3. Click *Register*.



Device Registration

Registration Status > **FortiCloud Account** > Registration Summary

Email:

Password:

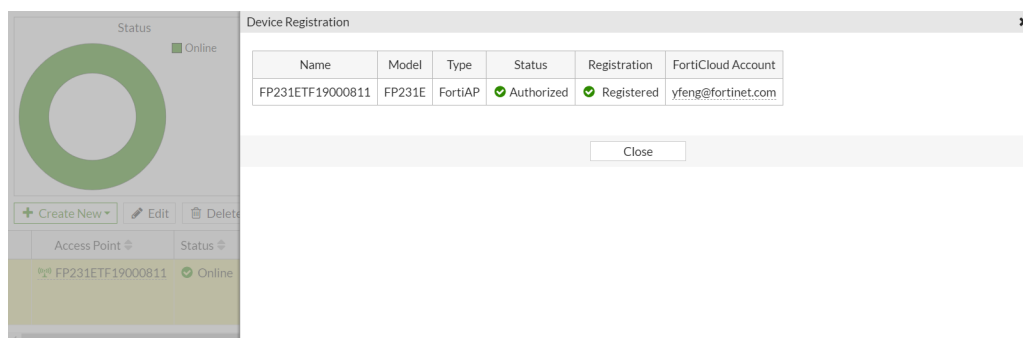
[Forgot your password?](#)

Country/Region:

Reseller:

4. Enter the FortiCloud account's email address and password, and select the country or region and reseller.
5. Click **Submit**.

The *Registration Summary* tab is shown. Registration can take 30 minutes. Once the FortiAP is registered, the FortiCloud account is listed.



Device Registration

Registration Status > FortiCloud Account > **Registration Summary**

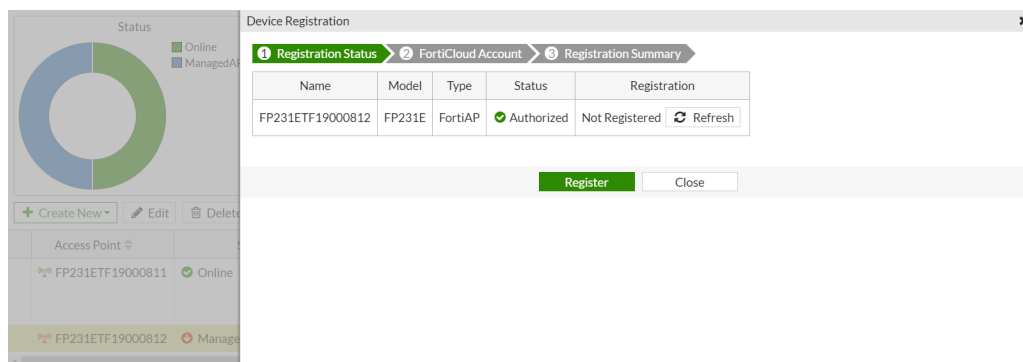
Name	Model	Type	Status	Registration	FortiCloud Account
FP231ETF19000811	FP231E	FortiAP	Authorized	Registered	yfeng@fortinet.com

6. Click **Close**.

### To register a FortiAP to FortiCloud when the FortiAP is authorized but offline:

1. Go to *WiFi & Switch Controller > Managed FortiAPs* and right click on the FortiAP.
2. Click **Registration**. This option is not available if the device is detected but not authorized.

The *Device Registration* pane opens, showing the device information and its registration status.



Device Registration

Registration Status > FortiCloud Account > **Registration Summary**

Name	Model	Type	Status	Registration
FP231ETF19000812	FP231E	FortiAP	Authorized	Not Registered <input type="button" value="Refresh"/>

3. Click **Register**.
4. Enter the FortiCloud account's email address and password, and select the country or region and reseller.

Device Registration

Registration Status > FortiCloud Account > Registration Summary

Email: abc@fortinet.com

Password: .....

Forgot your password?

Country/Region: Canada

Reseller: Unknown

Submit Cancel

5. Click **Submit**.

The **Registration Summary** tab is shown. The **Registration** status shows *Waiting for device to be online*.

Device Registration

Registration Status > FortiCloud Account > Registration Summary

Name	Model	Type	Status	Registration
FP231ETF19000812	FP231E	FortiAP	Authorized	Waiting for device to be online

Close

If the device comes online, the status changes to *Registering* while the device is being registered. Registration can take 30 minutes. Once the FortiAP is registered, the FortiCloud account is listed.

Device Registration

Registration Status > FortiCloud Account > Registration Summary

Name	Model	Type	Status	Registration
FP231ETF19000812	FP231E	FortiAP	Authorized	Timed out when waiting for device to be online <a href="#">Retry</a>

Close

If the device remains offline, the registration will eventually time out, and the status will show *Timed out when waiting for device to be online* and the **Retry** button can be clicked to try registering again.

6. Click **Close**.

**To view the FortiAP registration status:**

1. Go to **WiFi & Switch Controller > Managed FortiAPs** and right click on the FortiAP.
2. Click **Diagnostics and Tools**.

The *Registration* field shows the registration status.

The screenshot displays the 'Diagnostics and Tools - FP231ETF00000000' window. On the left, a status indicator shows a green circle with a checkmark. The main panel shows the following details:

- Serial Number:** FP231ETF00000000
- Base MAC Address:** 04:d5:90:90:38
- Status:** ✔
- Country/Region:** US
- Connected Via:** internal11
- IPv4 Address:** 10.2.120.2
- Uptime:** 13m
- Version:** v6.4
- Registration:** Registered

Below the details, there are tabs for 'Radios', 'Clients', 'Interfering SSIDs', 'Logs', 'CLI Access', 'Spectrum Analysis', and 'VLAN Probe'. The 'Radios' tab is active, showing a table with columns for Radio 1 - 2.4 GHz, Radio 2 - 5 GHz, and Radio 3.

	Radio 1 - 2.4 GHz	Radio 2 - 5 GHz	Radio 3
Mode	AP	AP	Monitor
SSID	All Tunnel Mode SSIDs	fortinet (test-yvonne)	N/A
Clients	0	0	0

## Add fields for wireless DHCP logs - 6.4.3

The following fields have been added to wireless DHCP logs:

- DHCP server MAC address
- Default gateway
- Subnet
- DNS server

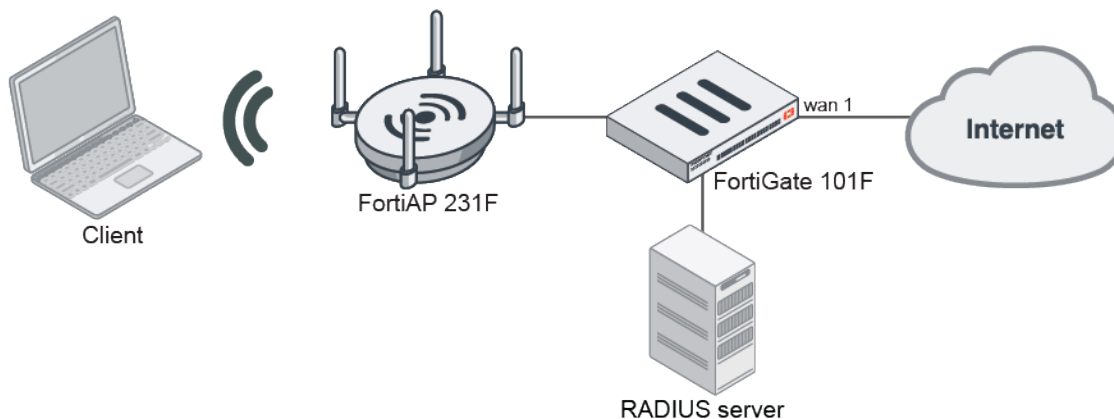
### Sample log:

```
date=2020-09-30 time=11:49:18 eventtime=1601491758459118834 tz="-0700" logid="0104043667"
type="event" subtype="wireless" level="notice" vd="root" logdesc="DHCP server sent DHCP ACK"
sn="FP423E3X16000020" ap="FP423E3X16000020" vap="123123" ssid="123123"
stamac="e0:5f:45:b3:84:70" security="WPA2 Personal" encryption="AES" action="DHCP-ACK"
reason="N/A" msg="DHCP ACK for IP 192.168.100.20 from server 192.168.100.1 with MAC
90:6c:ac:4e:47:b8 for client e0:5f:45:b3:84:70 from router 192.168.100.1 on subnet
255.255.255.0 with dns 10.1.1.1" remotewtptime="190.10544"
```

```
date=2020-09-30 time=11:49:17 eventtime=1601491757459960887 tz="-0700" logid="0104043664"
type="event" subtype="wireless" level="notice" vd="root" logdesc="DHCP server sent DHCP
OFFER" sn="FP423E3X16000020" ap="FP423E3X16000020" vap="123123" ssid="123123"
stamac="e0:5f:45:b3:84:70" security="WPA2 Personal" encryption="AES" action="DHCP-OFFER"
reason="N/A" msg="DHCP OFFER of IP 192.168.100.20 from server 192.168.100.1 with MAC
90:6c:ac:4e:47:b8 for client e0:5f:45:b3:84:70 from router 192.168.100.1 on subnet
255.255.255.0 with dns 10.1.1.1" remotewtptime="188.997518"
```

## Dynamic VLAN assignment using RADIUS attribute string - 6.4.6

With the Tunnel-Private-Group-Id RADIUS attribute, a wireless controller can now accept a VLAN name as a string, and match the VLAN sub-interface attached to a VAP interface when dynamically assigning a VLAN. Users logging into an SSID can be dynamically assigned to the proper VLAN based on the VLAN configurations in RADIUS for the particular user. Previously, only a numeric value was supported.



### To dynamically assign the VLAN using the RADIUS attribute string:

1. Configure the SSID with RADIUS authentication and dynamic VLAN enabled:

```

config wireless-controller vap
  edit "wifi.fap.02"
    set ssid "wifi-ssid.fap.02"
    set security wpa2-only-enterprise
    set auth radius
    set radius-server "peap"
    set schedule "always"
    set dynamic-vlan enable
  next
end

```

2. Configure the VLAN sub-interface:

```

config system interface
  edit "wifi2-vlan100"
    set vdom "vdom1"
    set ip 10.100.80.1 255.255.255.0
    set device-identification enable
    set role lan
    set snmp-index 28
    set interface "wifi.fap.02"
    set vlanid 100
  next
end

```

3. Configure the DHCP server:

```

config system dhcp server
  edit 7
    set dns-service default
    set default-gateway 10.100.80.1
    set netmask 255.255.255.0
    set interface "wifi2-vlan100"
    config ip-range
      edit 1
        set start-ip 10.100.80.2
        set end-ip 10.100.80.254
      next
    next
  end

```

```

    next
end

```

4. In FreeRADIUS, create a user account with the Tunnel-Private-Group-Id attribute set to the VLAN sub-interface:

```

user0100 Cleartext-Password := "123456"
        Tunnel-Type = "VLAN",
        Tunnel-Medium-Type = "IEEE-802",
        Session-Timeout=180,
        Tunnel-Private-Group-Id = wifi2-vlan100

```

5. Verify the client connection in FortiOS:

```

# diagnose wireless-controller wlac -d sta online
  vf=1 wtp=1 rId=2 wlan=wifi.fap.02 vlan_id=100 ip=10.100.80.2 ip6=:
mac=**:**:**:**:** vci= host=fosqa-PowerEdge-R210 user=user0100 group=peap signal=-15
noise=-95 idle=5 bw=0 use=6 chan=149 radio_type=11AX_5G security=wpa2_only_enterprise
mpsk= encrypt=aes cp_authed=no online=yes mimo=2

```

## Switch controller

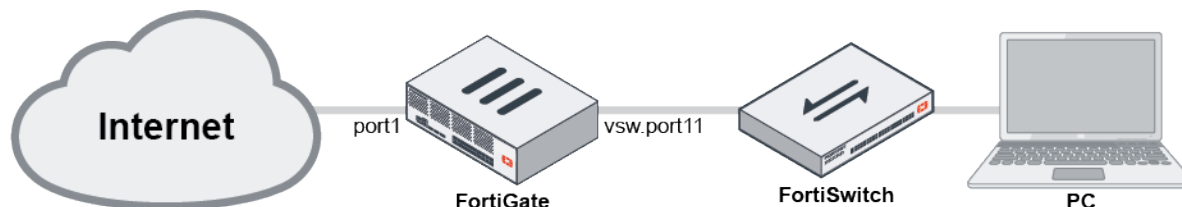
This section includes information about switch controller related new features:

- [Switch controller - quarantine by redirect on page 434](#)
- [VLAN interface templates for FortiSwitch devices on page 436](#)
- [Improved FortiSwitch support on page 440](#)
- [GUI support for FortiLink groups on page 440](#)
- [FortiSwitch link status visibility improvements on page 441](#)
- [SNMP queries to the FortiGate Switch Controller for FortiSwitch and port information 6.4.2 on page 442](#)
- [Allow FortiSwitch Trunk mode selection on FortiGate 6.4.2 on page 444](#)
- [Send multiple RADIUS attribute values in a single RADIUS Access-Request 6.4.2 on page 445](#)
- [ECN configuration for managed FortiSwitch devices 6.4.2 on page 445](#)
- [Configure PTP Transparent Clock mode for managed FortiSwitch devices 6.4.2 on page 446](#)
- [Inter-operability with per instance RSTP 802.1w 6.4.2 on page 447](#)
- [FortiGate HA between remote sites over managed FortiSwitches 6.4.2 on page 447](#)
- [Register FortiSwitch to FortiCloud from the GUI 6.4.2 on page 452](#)
- [GUI support for multiple FortiLink interfaces 6.4.2 on page 455](#)
- [Switch controller option to control the sources used to update the user device list 6.4.2 on page 459](#)
- [Log sub-category for switch controller 6.4.3 on page 460](#)
- [Configure LLDP settings on a switch port that is leased to a tenant VDOM 6.4.3 on page 461](#)
- [Add a RADIUS timeout VLAN to a security policy 6.4.3 on page 462](#)
- [Add option to enable flow control and pause metering 6.4.3 on page 462](#)
- [Allow switch controller to set source IP for outbound connections 6.4.3 on page 463](#)
- [Enable IoT background scanning 6.4.3 on page 464](#)

## Switch controller - quarantine by redirect

Quarantine by redirect makes the FortiSwitch redirect traffic from the quarantined host to the FortiGate, keeping the device on its original network. This is the default quarantine mode.

Quarantine by VLAN, which moves the device from the normal switch VLAN to the quarantine VLAN, can be complicated for administrators that use DHCP or static IP address assignments. When a device is sent to quarantine, its IP address is no longer valid for the quarantined VLAN segment, making it difficult to perform remediation on the device.



In this example, the PC can access the internet when there is an allowed policy from interface vsw.port11 to port1 (called *PC to Internet*). When the PC is quarantined, a firewall address is automatically created for the PC, which is added to an automatically created address group called *QuarantinedDevices*. A policy (called *quarantine*) is created that applies to this address group and blocks traffic from the PC to the internet.

The FortiSwitch configuration is done automatically after the FortiGate configured.

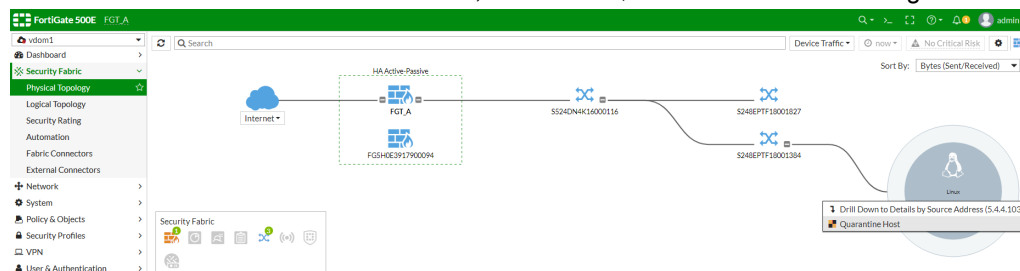
### To configure the quarantine mode:

```

config switch-controller global
    set quarantine-mode {by-vlan | by-redirect (default)}
end
  
```

### To quarantine an active device, based on the device's MAC address, in the GUI:

1. Go to *Security Fabric > Physical Topology* or *Security Fabric > Logical Topology*.
2. Mouse over the bubble of an active device, and select *Quarantine Host* from the right-click menu.



3. Click *OK* in the *Quarantine Host* page to quarantine the device. Firewall addresses and an address group (*QuarantinedDeivces*) are automatically added for the quarantined devices.



Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSLVPN tunnel Interface (sslvdsm1)	Visible	2
all	Subnet	0.0.0.0/0		Visible	5
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0
qtn.mac_00:00:00:00:00:00	Device (MAC Address)	00:00:00:00:00:00		Visible	1
qtn.mac_00:0c:29:d4:4f:3c	Device (MAC Address)	00:0c:29:d4:4f:3c		Visible	1
wildcard.dropbox.com	FQDN	*dropbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	1
G Suite	Address Group	gmail.com wildcard.google.com		Visible	0
Microsoft Office 365	Address Group	login.microsoftonline.com login.microsoft.com login.windows.net		Visible	0
QuarantinedDevices	Address Group	qtn.mac_00:00:00:00:00:00 qtn.mac_00:0c:29:d4:4f:3c		Visible	2

4. Go to **Policy & Objects > Firewall Policy** and create a policy to block traffic from quarantined devices to the internet.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
3	quarantine	QuarantinedDevices	all	always	ALL	DENY			Disabled	160.04 MB
2	PC to Internet	all	all	always	ALL	ACCEPT	Enabled	no-inspection	Disabled	398.50 kB

To quarantine an active device, based on the device's MAC address, in the CLI:

```
config user quarantine
  set traffic-policy quarantine
  set firewall-groups "QuarantinedDevices"
config targets
  edit "manual-qtn-1"
    set description "Manually quarantined"
  config macs
    edit 00:0c:29:d4:4f:3c
      set description "manual-qtn"
      set drop disable
    next
  end
next
end
```

Firewall addresses are automatically created for the quarantined MAC address, and the addresses are added to the *QuarantinedDevices* address group:

```
# show firewall address | grep -f qtn
config firewall address
  edit "qtn.mac_00:00:00:00:00:00" <---
    set uuid 9069e73c-3c6e-51ea-28d4-b807167fdcb7
    set type mac
    set comment "Quarantine dummy MAC to keep the addrgrp"
  next
  edit "qtn.mac_00:0c:29:d4:4f:3c" <---
    set uuid 869847ce-3c84-51ea-59c2-964152415e22
```

```
        set type mac
        set start-mac 00:0c:29:d4:4f:3c
        set end-mac 00:0c:29:d4:4f:3c
        set comment "Quarantine MAC"
    next
end

# show firewall addrgrp | grep -f Quarantined
config firewall addrgrp
    edit "QuarantinedDevices" <---
        set uuid 9069d332-3c6e-51ea-17e1-cab3dd4dde6c
        set member "qtn.mac_00:00:00:00:00:00" "qtn.mac_00:0c:29:d4:4f:3c"
    next
end
```

### To view the automatic configuration changes on the FortiSwitch:

```
config switch quarantine
    edit 00:0c:29:d4:4f:3c
        set acl-id 2
        set cos-queue 0
        set description "manual-qtn "
        set policer 1
    next
end
config switch acl ingress
    edit 2
        config action
            set cos-queue 0
            set count enable
            set policer 1
        end
        config classifier
            set src-mac 00:0c:29:d4:4f:3c
        end
        set ingress-interface-all enable
    next
end
```

## VLAN interface templates for FortiSwitch devices

You can create configuration templates that define the VLAN interfaces and are applied to new FortiSwitch devices when they are discovered and managed by the FortiGate.

For each VDOM, you can create templates, and then assign those templates to the automatically created switch VLAN interfaces for six types of traffic. The network subnet that is reserved for the switch controller can also be customized.

To ensure that switch VLAN interface names are unique for each system, the following naming rules are used:

- root VDOM: the interface names are the same as the template names.
- other VDOMs: the interface name is created from the template name and the SNMP index of the interface. For example, if the template name is *quarantined* and the SNMP index is 29, then the interface name is *quarantined.29*.

You can also customize the FortiLink management VLAN per FortiLink interface:

```

config system interface
    edit <fortilink interface>
        set fortilink enable
        set switch-controller-mgmt-vlan <integer>
    next
end

```

The management VLAN can be a number from 1 to 4094. the default value is 4094.

## Create VLAN interface templates

### To configure the VLAN interface templates:

```

config switch-controller initial-config template
    edit <template_name>
        set vlanid <integer>
        set ip <ip/netmask>
        set allowaccess {options}
        set auto-ip {enable | disable}
        set dhcp-server {enable | disable}
    next
end

```

<template_name>	The name, or part of the name, of the template.
vlanid <integer>	The unique VLAN ID for the type of traffic the template is assigned to (1 - 4094, default = 4094)
ip <ip/netmask>	The IP address and subnet mask of the switch VLAN interface. This can only be configured when <code>auto-ip</code> is disabled.
allowaccess {options}	The permitted types of management access to this interface.
auto-ip {enable   disable}	When enabled, the switch-controller will pick an unused 24 bit subnet from the <code>switch-controller-reserved-network</code> (configured in <code>config system global</code> ).
dhcp-server {enable   disable}	When enabled, the switch-controller will create a DHCP server for the switch VLAN interface

### To assign the templates to the specific traffic types:

```

config switch-controller initial-config vlans
    set default-vlan <template>
    set quarantine <template>
    set rspan <template>
    set voice <template>
    set video <template>
    set nac <template>
end

```

default-vlan <template>	Default VLAN assigned to all switch ports upon discovery.
quarantine <template>	VLAN for quarantined traffic.

rspan <template>	VLAN for RSPAN/ERSPAN mirrored traffic.
voice <template>	VLAN dedicated for voice devices.
video <template>	VLAN dedicated for video devices.
nac <template>	VLAN for NAC onboarding devices.

### To configure the network subnet that is reserved for the switch controller:

```
config system global
    set switch-controller-reserved-network <ip/netmask>
end
```

The default value is 169.254.0.0 255.255.0.0.

## Example

In this example, six templates are configured with different VLAN IDs. Except for the default template, all of them have DHCP server enabled. When a FortiSwitch is discovered, VLANs and the corresponding DHCP servers are automatically created.

### To configure six templates and apply them to VLAN traffic types:

```
config switch-controller initial-config template
    edit "default"
        set vlanid 1
        set auto-ip disable
    next
    edit "quarantine"
        set vlanid 4093
        set dhcp-server enable
    next
    edit "rspan"
        set vlanid 4092
        set dhcp-server enable
    next
    edit "voice"
        set vlanid 4091
        set dhcp-server enable
    next
    edit "video"
        set vlanid 4090
        set dhcp-server enable
    next
    edit "onboarding"
        set vlanid 4089
        set dhcp-server enable
    next
end

config switch-controller initial-config vlans
    set default-vlan "default"
    set quarantine "quarantine"
    set rspan "rspan"
```

```
set voice "voice"
set video "video"
set nac "onboarding"
end
```

**To see the automatically created VLANs and DHCP servers:**

```
show system interface
edit "default"
    set vdom "root"
    set snmp-index 24
    set switch-controller-feature default-vlan
    set interface "fortilink"
    set vlanid 1
next
edit "quarantine"
    set vdom "root"
    set ip 169.254.11.1 255.255.255.0
    set description "Quarantine VLAN"
    set security-mode captive-portal
    set replacemsg-override-group "auth-intf-quarantine"
    set device-identification enable
    set snmp-index 25
    set switch-controller-access-vlan enable
    set switch-controller-feature quarantine
    set color 6
    set interface "fortilink"
    set vlanid 4093
next
...
end

show system dhcp server
edit 2
    set dns-service local
    set ntp-service local
    set default-gateway 169.254.1.1
    set netmask 255.255.255.0
    set interface "fortilink"
    config ip-range
        edit 1
            set start-ip 169.254.1.2
            set end-ip 169.254.1.254
        next
    end
    set vci-match enable
    set vci-string "FortiSwitch" "FortiExtender"
next
edit 3
    set dns-service default
    set default-gateway 169.254.11.1
    set netmask 255.255.255.0
    set interface "quarantine"
    config ip-range
        edit 1
            set start-ip 169.254.11.2
            set end-ip 169.254.11.254
```

```

    next
  end
  set timezone-option default
next
...
end

```

## Improved FortiSwitch support

The number of managed FortiSwitch devices has increased in some FortiGate E models.

FortiGate model	Number of managed FortiSwitches
200E, 201E	64 (from 32)
300E, 301E, 400E, 401E	72 (from 48)
500E, 501E	72 (from 48)
600E, 601E	96 (from 64)
2000E, 2500E	196 (from 128)

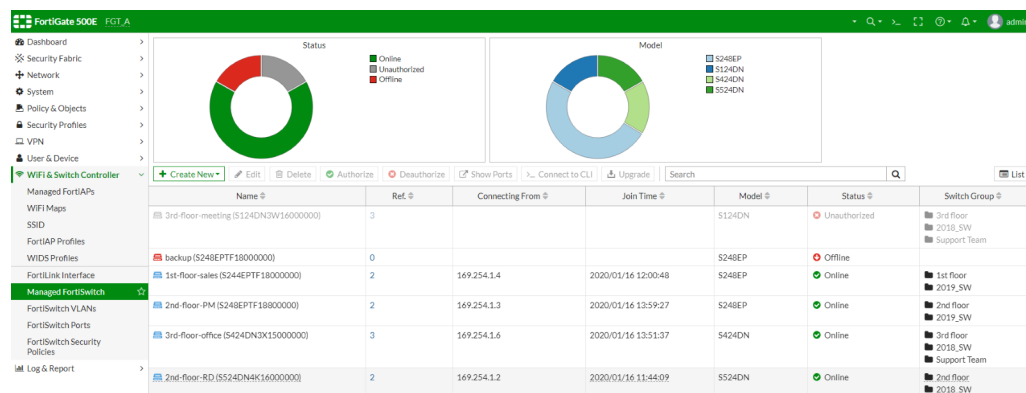
## GUI support for FortiLink groups

The *Managed FortiSwitch* page includes two new display options: *List* view and *Group* view.

### To view the display options:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. In the toolbar menu, use the dropdown list to switch between views. The previous *Managed FortiSwitch Topology* is under *Topology* view.

#### List view:



#### Group view:

Name	Ref	Members
1st floor	0	1st-floor-sales (S244EPTF18000000)
2nd floor	0	2nd-floor-PM (S248EPTF18800000)
3rd floor	0	2nd-floor-RD (S524DN4K16000000)
2019_SW	0	3rd-floor-meeting (S124DN3W16000000)
2019_SW	0	3rd-floor-office (S424DN3K15000000)
Support Team	0	2nd-floor-RD (S524DN4K16000000)

## FortiSwitch link status visibility improvements

The *Managed FortiSwitch* page topology view has been improved to illustrate the FortiSwitch link status. The following changes have been made in the GUI:

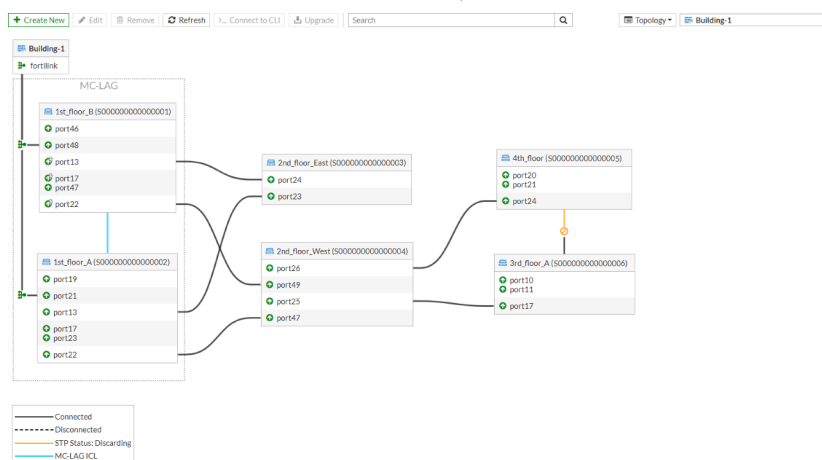
- The FortiSwitch faceplate was replaced with a box that displays ports used for FortiLink management.
- Hovering over switch ports and the links between switches displays a tooltip, which shows the port on both sides of a link.
- The MC-LAG ICL and STP discarding statuses are color coded.
- The MC-LAG cluster is enclosed in a box with an *MC-LAG* label.
- A dropdown list is available to switch between *Managed FortiSwitch* pages of downstream Security Fabric members.
- FortiSwitch names and serial numbers can be used as parameters in the *Search* function.

In the following example, FG-500E (Building-1) is the Fabric root device and FG-90E (Building-2) is the downstream device. There are six FortiSwitches managed by FG-500E and two FortiSwitches managed by FG-90E.

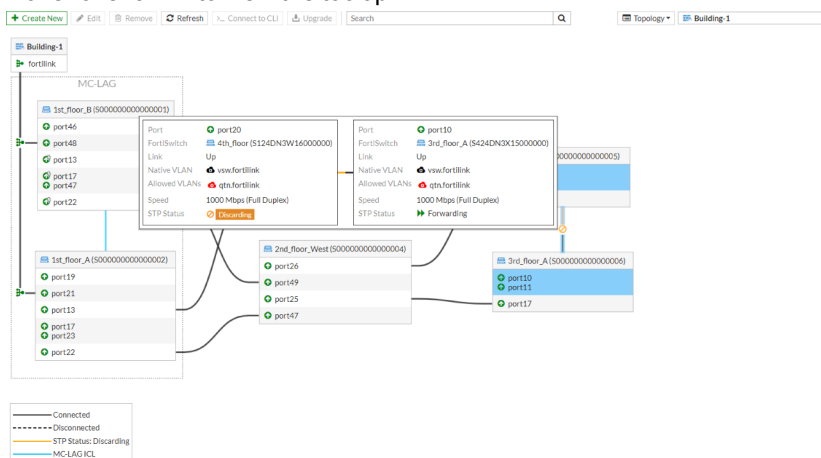
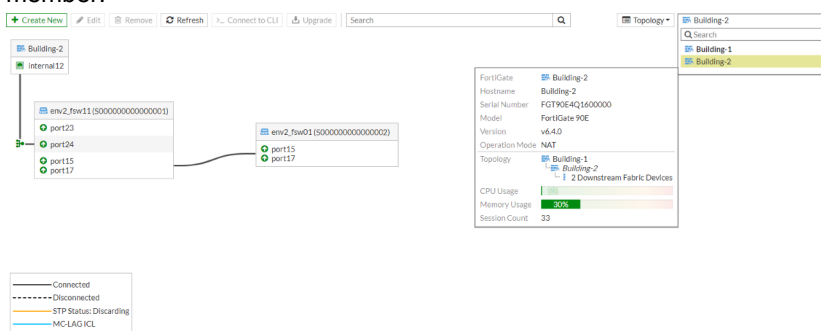
### To view the FortiSwitch link status in the GUI:

- On the root device, go to *WiFi & Switch Controller > Managed FortiSwitch*.
- In the toolbar menu, select *Topology* from the dropdown list.

The MC-LAG cluster is enclosed in a box, and the MC-LAG ICL and STP discarding statuses are color coded:



## 3. Hover over a link to view the tooltip.

4. In the toolbar menu, use the dropdown list to view the *Managed FortiSwitch* page of the downstream Security Fabric member.

## SNMP queries to the FortiGate Switch Controller for FortiSwitch and port information - 6.4.2

Two new tables are added to the FortiOS Enterprise MIB:

- *FgSwDeviceEntry*: Details about connected FortiSwitch devices.
- *FgSwPortEntry*: Switch port related information.

### FgSwDeviceEntry

Table added to the FortiGate SNMP MIB file:

```
/ OID: FORTINET-FORTIGATE-
MIB:fortinet.fnFortiGateMib.fgSw.fgSwDeviceInfo.fgSwDeviceTable.fgSwDeviceEntry
1.3.6.1.4.1.12356.101.24.1.1.1 /
```

```
FgSwDeviceEntry ::= SEQUENCE {
    fgSwDevicePlatform FnIndex,
    fgSwDeviceId FnIndex,
    fgSwDeviceSerialNum DisplayString,
    fgSwDeviceName DisplayString,
    fgSwDeviceVersion DisplayString,
    fgSwDeviceAuthorized FgSwDeviceAuthorizedType,
```



```

    fgSwDeviceStatus INTEGER,
    fgSwDeviceJoinTime Gauge32,
    fgSwDeviceIp IpAddress,
    fgSwDeviceFlag DisplayString
}

```

### SNMP response from the FortiGate:

```

# snmpwalk -v2c -c fortilink 172.16.200.1 1.3.6.1.4.1.12356.101.24.1.1.1
iso.3.6.1.4.1.12356.101.24.1.1.1.3.1.18.16000116 = STRING: "S524DN4K16000116"
iso.3.6.1.4.1.12356.101.24.1.1.1.4.1.18.16000116 = ""
iso.3.6.1.4.1.12356.101.24.1.1.1.5.1.18.16000116 = STRING: "v6.4.1"
iso.3.6.1.4.1.12356.101.24.1.1.1.6.1.18.16000116 = INTEGER: 2
iso.3.6.1.4.1.12356.101.24.1.1.1.7.1.18.16000116 = INTEGER: 1
iso.3.6.1.4.1.12356.101.24.1.1.1.8.1.18.16000116 = Gauge32: 1592346680
iso.3.6.1.4.1.12356.101.24.1.1.1.9.1.18.16000116 = IpAddress: 169.254.1.2
iso.3.6.1.4.1.12356.101.24.1.1.1.10.1.18.16000116 = STRING: "-"

```

## FgSwPortEntry

### Table added to the FortiGate SNMP MIB file:

```

/ OID: FORTINET-FORTIGATE-
MIB:fortinet.fnFortiGateMib.fgSw.fgSwPortInfo.fgSwPortTable.fgSwPortEntry
1.3.6.1.4.1.12356.101.24.2.1.1 /

```

```

FgSwPortEntry ::= SEQUENCE {
    fgSwPortSwitchPlatform FnIndex,
    fgSwPortSwitchId FnIndex,
    fgSwPortNum FnIndex,
    fgSwPortSwitchSerialNum DisplayString,
    fgSwPortName DisplayString,
    fgSwPortStatus INTEGER,
    fgSwPortSpeedDuplex DisplayString,
    fgSwPortNativeVlan Integer32,
    fgSwPortAllowedVlan DisplayString,
    fgSwPortUntaggedVlan DisplayString,
    fgSwPortPOE INTEGER,
    fgSwPortPOEStatus INTEGER,
    fgSwPortPOEState DisplayString,
    fgSwPortPOEPower DisplayString
}

```

### SNMP response from the FortiGate:

```

# snmpwalk -v2c -c fortilink 172.16.200.1 1.3.6.1.4.1.12356.101.24.2.1.1
iso.3.6.1.4.1.12356.101.24.2.1.1.4.1.18.16000116.1 = STRING: "S524DN4K16000116"
...
iso.3.6.1.4.1.12356.101.24.2.1.1.4.1.18.16000116.30 = STRING: "S524DN4K16000116"
iso.3.6.1.4.1.12356.101.24.2.1.1.5.1.18.16000116.1 = STRING: "port1"
...
iso.3.6.1.4.1.12356.101.24.2.1.1.5.1.18.16000116.30 = STRING: "port30"
iso.3.6.1.4.1.12356.101.24.2.1.1.6.1.18.16000116.1 = INTEGER: 1
...

```

```

iso.3.6.1.4.1.12356.101.24.2.1.1.6.1.18.16000116.30 = INTEGER: 1
iso.3.6.1.4.1.12356.101.24.2.1.1.7.1.18.16000116.1 = STRING: "auto"
...
iso.3.6.1.4.1.12356.101.24.2.1.1.7.1.18.16000116.24 = STRING: "auto"
iso.3.6.1.4.1.12356.101.24.2.1.1.7.1.18.16000116.25 = STRING: "auto-module"
...
iso.3.6.1.4.1.12356.101.24.2.1.1.7.1.18.16000116.28 = STRING: "auto-module"
iso.3.6.1.4.1.12356.101.24.2.1.1.7.1.18.16000116.29 = STRING: "40000"
iso.3.6.1.4.1.12356.101.24.2.1.1.7.1.18.16000116.30 = STRING: "40000"
iso.3.6.1.4.1.12356.101.24.2.1.1.8.1.18.16000116.1 = INTEGER: 1
...
iso.3.6.1.4.1.12356.101.24.2.1.1.8.1.18.16000116.30 = INTEGER: 1
iso.3.6.1.4.1.12356.101.24.2.1.1.9.1.18.16000116.1 = STRING: "4093"
...
iso.3.6.1.4.1.12356.101.24.2.1.1.9.1.18.16000116.30 = STRING: "4093"
iso.3.6.1.4.1.12356.101.24.2.1.1.10.1.18.16000116.1 = STRING: "4093"
...
iso.3.6.1.4.1.12356.101.24.2.1.1.10.1.18.16000116.30 = STRING: "4093"
iso.3.6.1.4.1.12356.101.24.2.1.1.11.1.18.16000116.1 = INTEGER: 0
...
iso.3.6.1.4.1.12356.101.24.2.1.1.11.1.18.16000116.30 = INTEGER: 0
iso.3.6.1.4.1.12356.101.24.2.1.1.12.1.18.16000116.1 = INTEGER: 1
...
iso.3.6.1.4.1.12356.101.24.2.1.1.12.1.18.16000116.30 = INTEGER: 1
iso.3.6.1.4.1.12356.101.24.2.1.1.13.1.18.16000116.1 = STRING: "Disabled"
...
iso.3.6.1.4.1.12356.101.24.2.1.1.13.1.18.16000116.30 = STRING: "Disabled"
iso.3.6.1.4.1.12356.101.24.2.1.1.14.1.18.16000116.1 = STRING: "0.000000"
...
iso.3.6.1.4.1.12356.101.24.2.1.1.14.1.18.16000116.30 = STRING: "0.000000"

```

## Allow FortiSwitch Trunk mode selection on FortiGate - 6.4.2

In an LACP trunk, ports with the same negotiated speed are grouped into an aggregator. Setting the aggregator mode allows you to select the aggregator based on either the bandwidth or the number of links.

FortiSwitch version 6.4.0 and later are supported.

### To configure the aggregator mode for a FortiSwitch managed by FortiGate:

```

config switch-controller managed-switch
    edit <switch>
        config ports
            edit "trunk_server1"
                set aggregator-mode {bandwidth | count}
                set vlan "default.13"
                set type trunk
                set mac-addr 90:6c:ac:de:35:fe
                set mode lacp-active
                set members "port11" "port12"
            next
        end
    next
end

```

Where

bandwidth	The aggregator with the largest bandwidth is selected (default).
count	The aggregator with the largest number of ports is selected.

## Send multiple RADIUS attribute values in a single RADIUS Access-Request - 6.4.2

A managed FortiSwitch can be configured to send multiple RADIUS attribute values in a single RADIUS Access-Request. This option is configured per RADIUS user, and is set to `none` by default.

The available service type options are:

login	User should be connected to a host.
framed	User use Framed Protocol.
callback-login	User disconnected and called back.
callback-framed	User disconnected and called back, then a Framed Protocol.
outbound	User granted access to outgoing devices.
administrative	User granted access to the administrative unsigned interface.
nas-prompt	User provided a command prompt on the NAS.
authenticate-only	Authentication requested, and no authentication information needs to be returned.
callback-nas-prompt	User disconnected and called back, then provided a command prompt.
call-check	Used by the NAS in an Access-Request packet, Access-Accept to answer the call.
callback-administrative	User disconnected and called back, granted access to the admin unsigned interface.

**To configure a managed FortiSwitch to the RADIUS attributes login, framed, and authenticate-only all at the same time:**

```
config user radius
    edit "Radius_Server"
        set switch-controller-service-type login framed authenticate-only
        ....
    next
end
```

## ECN configuration for managed FortiSwitch devices - 6.4.2

Explicit Congestion Notification (ECN) allows ECN enabled endpoints to notify each other when they are experiencing congestion. It is supported on the following FortiSwitch models: 3032E, 3032D, 1048E, 1048D, 5xxD series, and 4xxE series.

On the FortiGate that is managing the compatible FortiSwitch, ECN can be enabled for each Class of Service (CoS) queue to enable packet marking to drop eligible packets. The command is only available when the dropping policy is weighted random early detection. It is disabled by default.

#### To configure FortiSwitch to enable ECN packet marking to drop eligible packets:

```
config switch-controller qos queue-policy
    edit "ECN_marking"
        set schedule round-robin
        set rate-by kbps
        config cos-queue
            edit "queue-0"
                set drop-policy weighted-random-early-detection
                set ecn enable
            next
            edit "queue-1"
            next
            edit "queue-2"
            next
            ...
        end
    next
end
```

## Configure PTP Transparent Clock mode for managed FortiSwitch devices - 6.4.2

For communicating timing precision between two ends, PTP Transparent Clock mode can be enabled to measure and adjust for packet delay. It is supported on the following FortiSwitch models: 3032E, 3032D, 1048E, 5xxD series, 4xxE series, 424D, 224E, and 224D.

On the FortiGate that is managing the compatible FortiSwitch, switch controller PTP settings and policies can be configured per VDOM. A PTP policy can also be selected for each FortiSwitch port.

#### To configure the switch controller PTP settings:

```
config switch-controller ptp settings
    set mode {default | transparent-e2e | transparent-p2p}
end
```

default	Disable the PTP function (default). Packets are forwarded with no action.
transparent-e2e	Enable end-to-end transparent clock.
transparent-p2p	Enable peer-to-peer transparent clock.

#### To configure a switch controller PTP policy:

```
config switch-controller ptp policy
    edit "default"
        set status enable
    next
end
```

**To set the PTP policy on a switch port:**

```
config switch-controller managed-switch
  edit "S524D000000000000"
    config ports
      edit "port1"
        set ptp-policy default
      next
    end
  next
end
```

## Inter-operability with per instance RSTP 802.1w - 6.4.2

Inter-operability with rapid Per-VLAN Spanning Tree plus (PVST+) can be enabled per port on managed FortiSwitch devices. It is disabled by default.

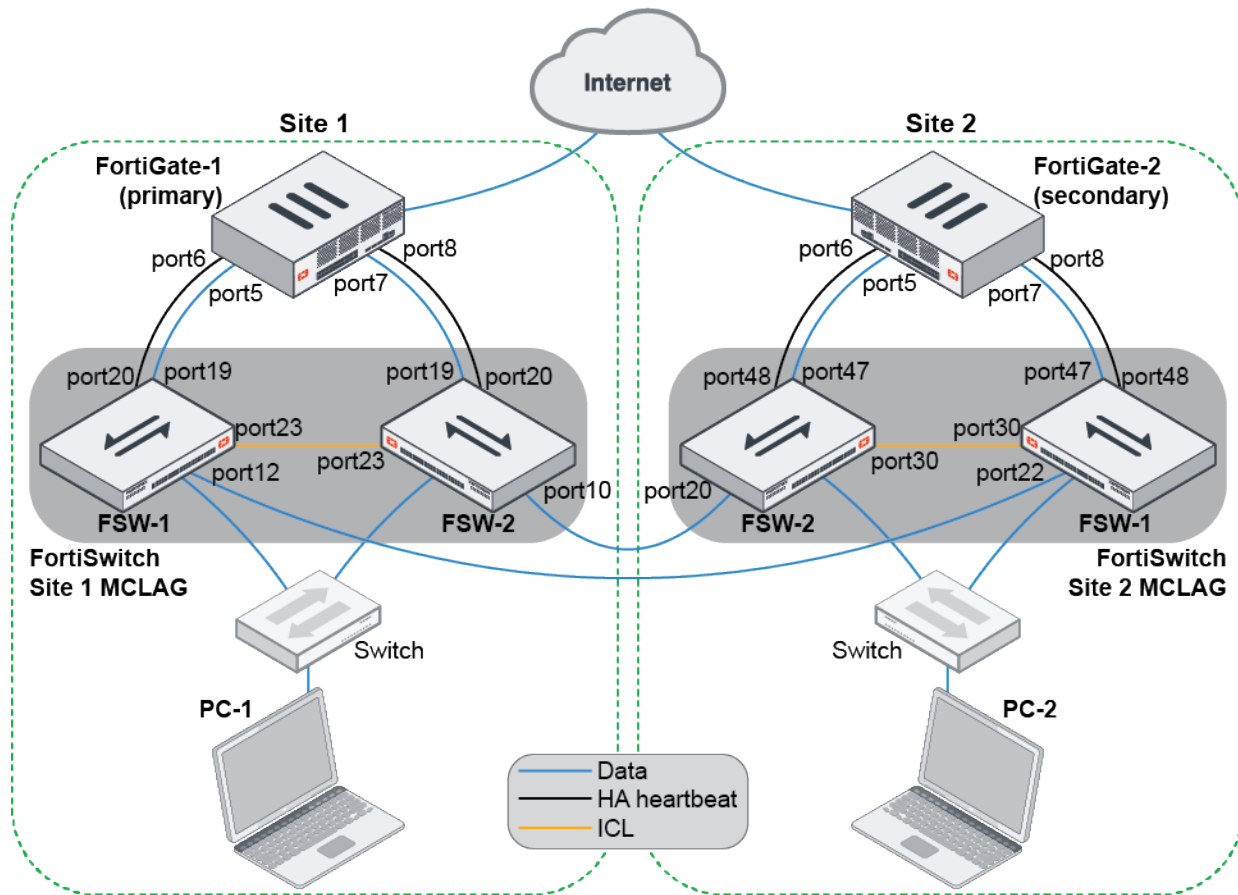
**To enable rapid PVST+ on port3 of a managed FortiSwitch:**

```
config switch-controller managed-switch
  edit "S524D000000000000"
    config ports
      edit "port3"
        set rpvt-port enable
      next
    end
  next
end
```

## FortiGate HA between remote sites over managed FortiSwitches - 6.4.2

In a multi-site FortiGate HA topology that uses managed FortiSwitches in a multi-chassis link aggregation group (MCLAG) to connect between sites, HA heartbeat signals can be sent through the switch layer of the FortiSwitches, instead of through back-to-back links between the heartbeat interfaces. This means that two fiber connections can be used, instead of four. The FortiSwitches can be different models, but must all support MCLAG and be running version 6.4.2 or later.

This example shows how to configure heartbeat VLANs to assign to the access ports that the heartbeat interfaces connect to, passing over the trunk between the FortiSwitches on the two sites.



FortiGate HA is with two FortiGates in separate locations and the switch layer connection between the FortiSwitches is used for the heartbeat signal.

#### To configure the example:

1. Disconnect the physical connections between Site 1 and Site 2:
  - Disconnect the cable on Site 1 FSW-1 port 12.
  - Disconnect the cable on Site 1 FSW-2 port 10.

## 2. Configure Site 1:

- a. On the FortiGate, go to *WiFi & Switch Controller > FortiLink Interface* and configure FortiLink:

- b. Go to *System > HA* and configure HA:
- Set the heartbeat ports to the ports that are connected to FortiSwitch.
  - Adjust the priority and enable override so that this FortiGate becomes the primary.

- c. Go to *WiFi & Switch Controller > FortiSwitch VLANs* and create a switch VLAN that is dedicated to the FortiGate HA heartbeats between the two FortiGates.

- d. Assign the native VLAN of the switch ports that are connected to the heartbeat ports to the created VLAN:
- Go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - In the *Native VLAN* column for the port, click the edit icon and select the *Heartbeat* VLAN.

Port	Trunk	Access Mode	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information
port10		Normal	Edge Port Spanning Tree Protocol	default	quarantine		
port11		Normal	Edge Port Spanning Tree Protocol	default	quarantine		
port12		Normal	Edge Port Spanning Tree Protocol	FS00000000000000			
port13		Normal	Edge Port Spanning Tree Protocol	default	quarantine		
port14		Normal	Edge Port Spanning Tree Protocol	default	quarantine		
port15		Normal	Edge Port Spanning Tree Protocol	default	quarantine		
port16		Normal	Edge Port Spanning Tree Protocol	default	quarantine		
port17		Normal	Edge Port Spanning Tree Protocol	default	quarantine		
port18		Normal	Edge Port Spanning Tree Protocol	default	quarantine		
port19		Normal	Edge Port Spanning Tree Protocol	FGT3HD9999000000			
port20		Normal	Edge Port Spanning Tree Protocol	Heartbeat	quarantine		

- e. On each FortiSwitch, enable MCLAG-ICL on the trunk port:

```
config switch trunk
    edit D243Z17000032-0
        set mclag-icl enable
    next
end
```

- Configure Site 2 the same as Site 1, except set the HA priority so that the FortiGate becomes the secondary.
- Disconnect the physical connections for FortiGate HA and FortiLink interfaces on Site 2:
  - Disconnect the cable on Site 2 FSW-1 ports 47 and 48.
  - Disconnect the cable on Site 2 FSW-2 ports 47 and 48.
- Connect cables between the FortiSwitch MCLAG in Site 1 and Site 2:
  - Connect a cable from Site 1 FSW-1 port 12 to Site 2 FSW-1 port 22.
  - Connect a cable from Site 1 FSW-2 port 10 to Site 2 FSW-2 port 20.



6. On all of the FortiSwitches, configure the `auto-isl-port-group`. The group must match on both sides.

a. Site 1 FSW-1:

Set `members` to the port that is connected to Site 2 FSW-1:

```
config switch auto-isl-port-group
  edit 1
    set members port12
  next
end
```

b. Site 1 FSW-2:

Set `members` to the port that is connected to Site 1 FSW-1:

```
config switch auto-isl-port-group
  edit 1
    set members port22
  next
end
```

c. Site 2 FSW-1:

Set `members` to the port that is connected to Site 2 FSW-2:

```
config switch auto-isl-port-group
  edit 1
    set members port10
  next
end
```

d. Site 2 FSW-2:

Set `members` to the port that is connected to Site 1 FSW-2:

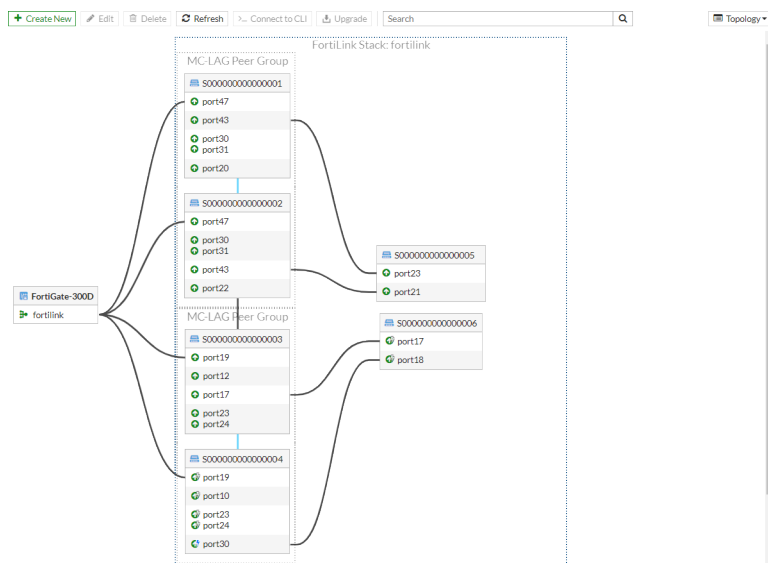
```
config switch auto-isl-port-group
  edit 1
    set members port20
  next
end
```

7. Connect the FortiGate HA and FortiLink interface connections on Site 2.

8. Configure a firewall policy and route for traffic so that the client can reach the internet.

9. Wait for HA to finish synchronizing and for all of the FortiSwitches to come online, then on FortiGate-1, go to *WiFi & Switch Controller > Managed FortiSwitch*.

The page should look similar to the following:



### To test the configuration to confirm what happens when there is a failover:

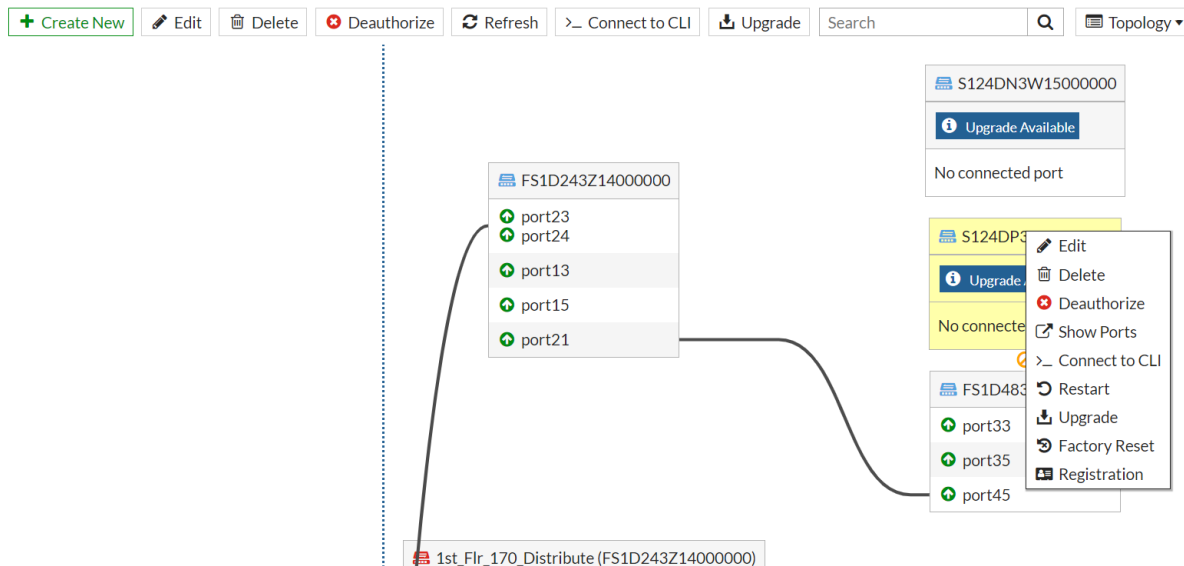
1. On both PC-1 and PC-2, access the internet and monitor traffic. The traffic should be going through the primary FortiGate.
2. Perform a continuous ping to an outside IP address, then reboot any one of the FortiSwitches. Traffic from both Site 1 and Site 2 to the internet should be recovered in approximately five seconds.
3. Perform a continuous ping to an outside IP address, then force an HA failover (see [Force HA failover for testing and demonstrations](#)). Traffic from both Site 1 and Site 2 to the internet should be recovered in approximately five seconds.
4. After an HA failover, on the new primary FortiGate, go to *WiFi & Switch Controller > Managed FortiSwitch*. The switch layer tiering will be changed so that the directly connected FortiSwitches are at the top of the topology.

## Register FortiSwitch to FortiCloud from the GUI - 6.4.2

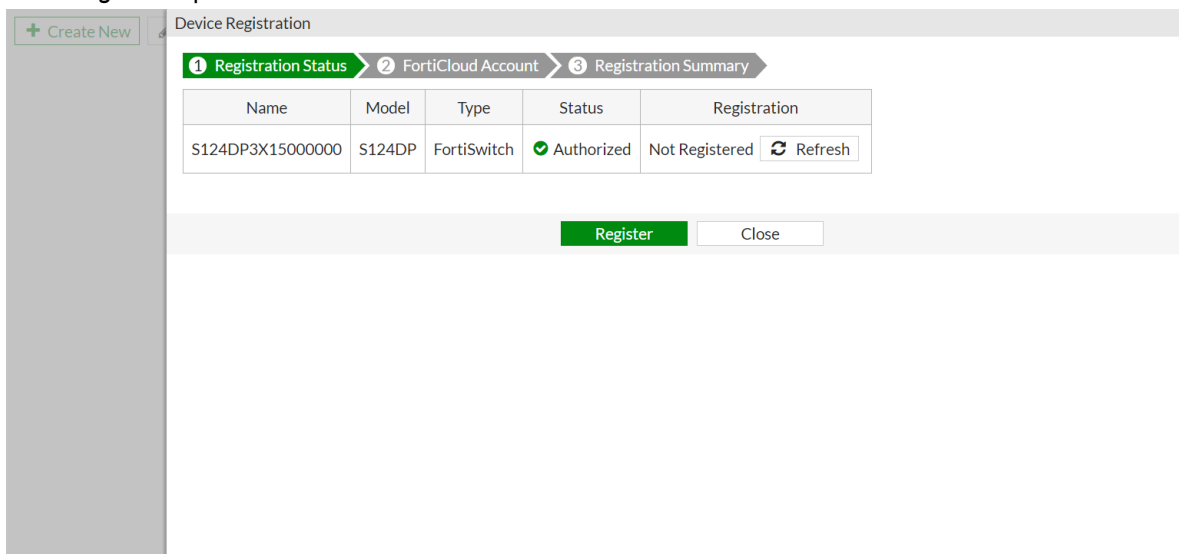
After authorizing a FortiSwitch, administrators can register the FortiSwitch to FortiCloud directly from the FortiOS GUI.

### To register the FortiSwitch in the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch* and ensure the *Topology* view is selected.
2. In the topology, right-click on an unregistered device and click *Registration*.



3. Complete the device registration wizard:
  - a. Click *Register* to proceed.



- b. Enter the FortiCloud account information and click *Submit*.

Device Registration

1 Registration Status > 2 FortiCloud Account > 3 Registration Summary

Email:

Password:

[Forgot your password?](#)

Country/Region:

Reseller:

The registration information is submitted to FortiCare, and FortiOS attempts to collect the registration status from FortiGuard. Since FortiGuard and FortiCare synchronize periodically, the registration status may not update immediately (it may take up to a few hours).

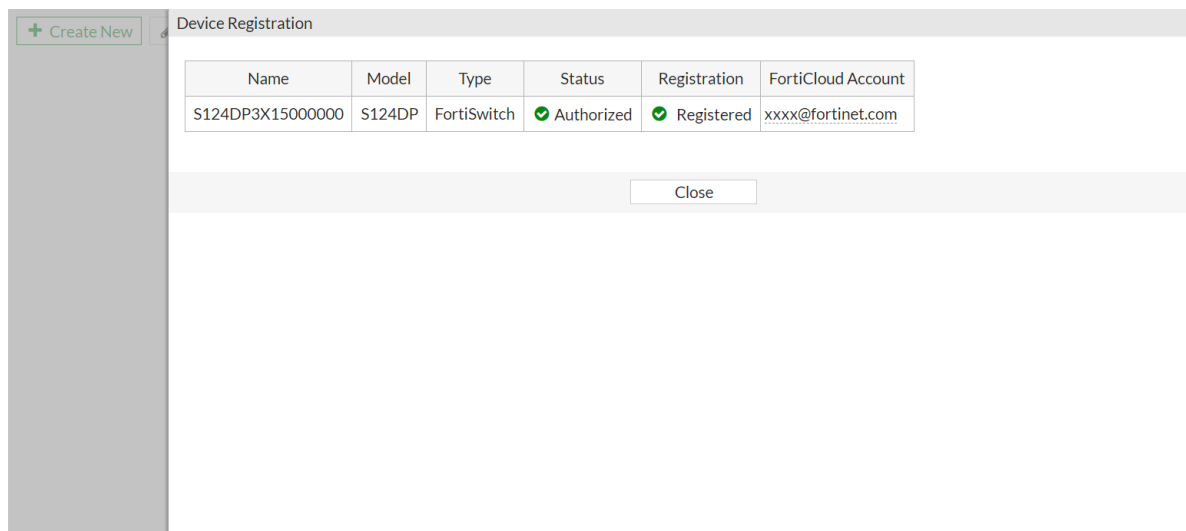
Device Registration

1 Registration Status > 2 FortiCloud Account > 3 Registration Summary

Name	Model	Type	Status	Registration
S124DP3X15000000	S124DP	FortiSwitch	Authorized	<input checked="" type="checkbox"/> Registration submitted, but information may need a moment to update. Please try again later. <input type="button" value="Refresh"/>

- c. Click *Close*.

4. After a while, go back to *WiFi & Switch Controller > Managed FortiSwitch*.
5. Right-click on the device and click *Registration*. The device is shown as *Registered* to the corresponding *FortiCloud* account.



### To register the FortiSwitch in the CLI:

```
# diagnose forticare direct-registration product-registration -N S124DP3X15000000 -a
xxxx@fortinet.com -p LDAP -T "CA" -R "other" -e 1
```

Account info:

```
contract_number=[] account_id=[xxxx@fortinet.com] password=[***]
reseller_id=0 reseller=[other]
first_name=[] last_name=[] company=[]
title=[] address=[] city=[]
state=[] state_code=[] country_code=0
post_code=[] phone=[] fax=[]
industry=[] industry_id=0 orgsize=[] orgsize_id=0
version=0 SN=[S124DP3X15000000] existing=1
```

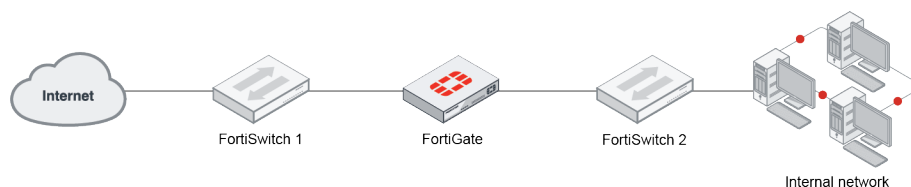
Prepare to register product into this account.

Do you want to continue? (y/n)y

Registration successful

## GUI support for multiple FortiLink interfaces - 6.4.2

The default command to restrict FortiLink interfaces to one interface has been removed. The GUI will display multiple FortiLink interfaces if more than one interface has FortiLink enabled from the CLI.



### To enable a physical or aggregate interface as a FortiLink in the CLI:

```
config system interface
  edit <port>
    set vdom "root"
    set fortilink enable
```

next

end

Multiple FortiLink interfaces are now displayed in the GUI.

**To create a FortiLink interface in the GUI:**

1. Go to *WiFi & Switch Controller > FortiLink Interface* and click *Create New*.
2. Configure the settings as needed.

3. Click *OK*. The new interface is displayed in the list.

Name	Type	Connected Devices	Administrative Access	DHCP Ranges	Ref.
newLink	802.3ad Aggregate		PING Security Fabric Connection	169.254.1.2-169.254.1.254	2
port10	Physical Interface	S248DP S248DP	PING Security Fabric Connection	10.9.8.2-10.9.8.254	12
port16	Physical Interface	S248DP	PING Security Fabric Connection		8

**GUI additions for WiFi & Switch Controller pages:**

The FortiLink interface can be selected from the dropdown on the following pages:

- *Managed FortiSwitch* list view:

Status

Model

Create New Edit Delete Upgrade >... Connect to CLI Search

List FortiLink port10

Name	Switch Group	Status	Model	Firmware Version	Connecting From	Join Time
S248DP3W15000000		Online	S248DP	S248DP-v3.6.3-build390.171020 (GA)	10.9.8.2	2020/07/24 18:18:35

- Managed FortiSwitch group view:

<div><div>+ Create New</div><div>Edit</div><div>Delete</div><div>Upgrade</div><div>Search</div><div>Q</div></div> <div><div>Group</div><div>FortiLink</div><div>port10</div></div>	
Name	Members
<div>fsw-group</div>	<div><div><div>S248</div><div></div></div><div><div>S248</div><div></div></div></div>

- FortiSwitch VLANs:

+ Create New

Edit

Delete

Search

Q

FortiLink

port10

Name	VLAN ID	IP	Administrative Access	Ref.
default	1	0.0.0.0/0.0.0		99
quarantine	4093	169.254.11.1/255.255.255.0		101
voice	4091	169.254.12.1/255.255.255.0		1
video	4090	169.254.13.1/255.255.255.0		1
rspan	4092	169.254.14.1/255.255.255.0		1
onboarding	4089	169.254.15.1/255.255.255.0		3

- FortiSwitch Ports:

+ Create New		Edit	Delete	Search			Port	Trunk	Faceplates	FortiLink	port10
Port	Trunk	Access Mode	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information	DHCP Snooping	Transceiver		
S248DP3W15000000											
port1		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port2		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port3		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port4		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port5		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port6		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port7		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port8		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port9		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port10		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port11		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port12		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port13		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port14		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted			
port15		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Powered		Untrusted		0% 100	

- FortiSwitch NAC Policies:

+ Create New

Edit

Delete

Search

Q

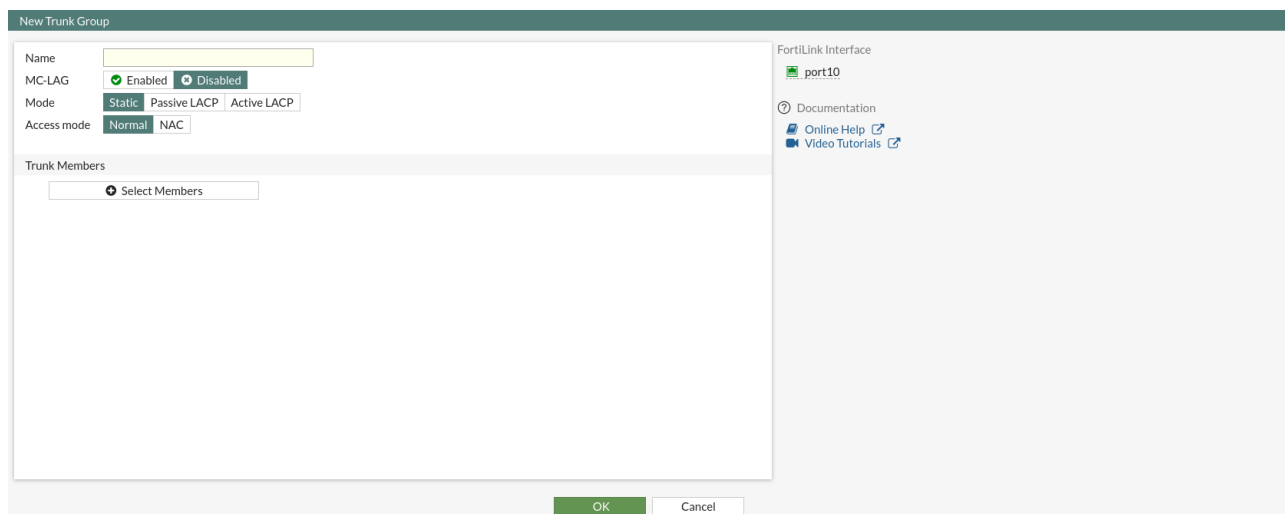
View Matched Devices

FortiLink

port10

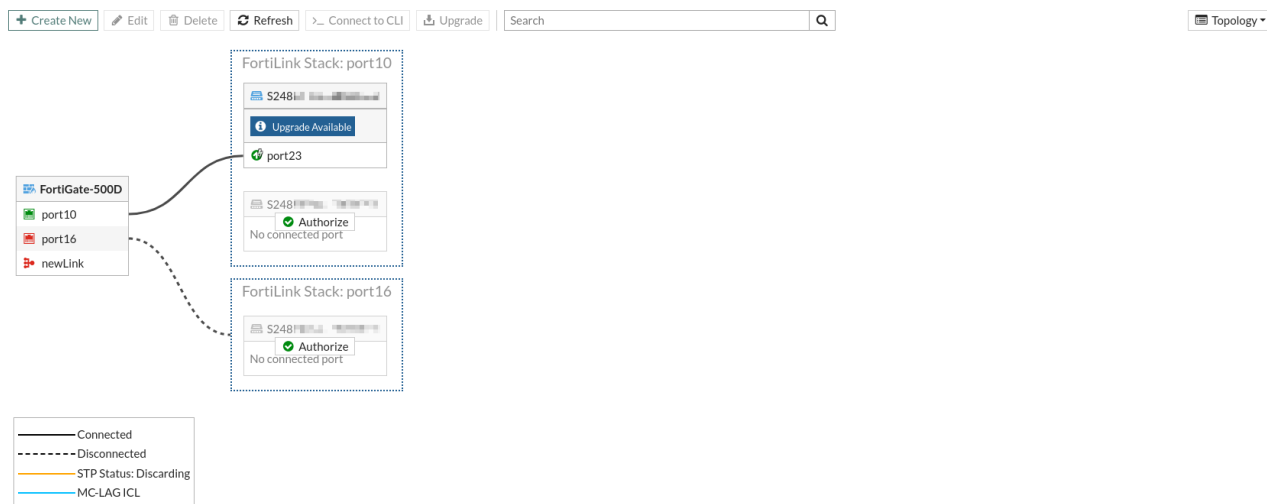
Name	Patterns	Assign	Matched Devices	Ref.
new		802.1X 802-1X-policy-default		0
Onboarding VLAN		VLAN onboarding		

When creating a new trunk group, the FortiLink interface is visible in the gutter:



### Topology views:

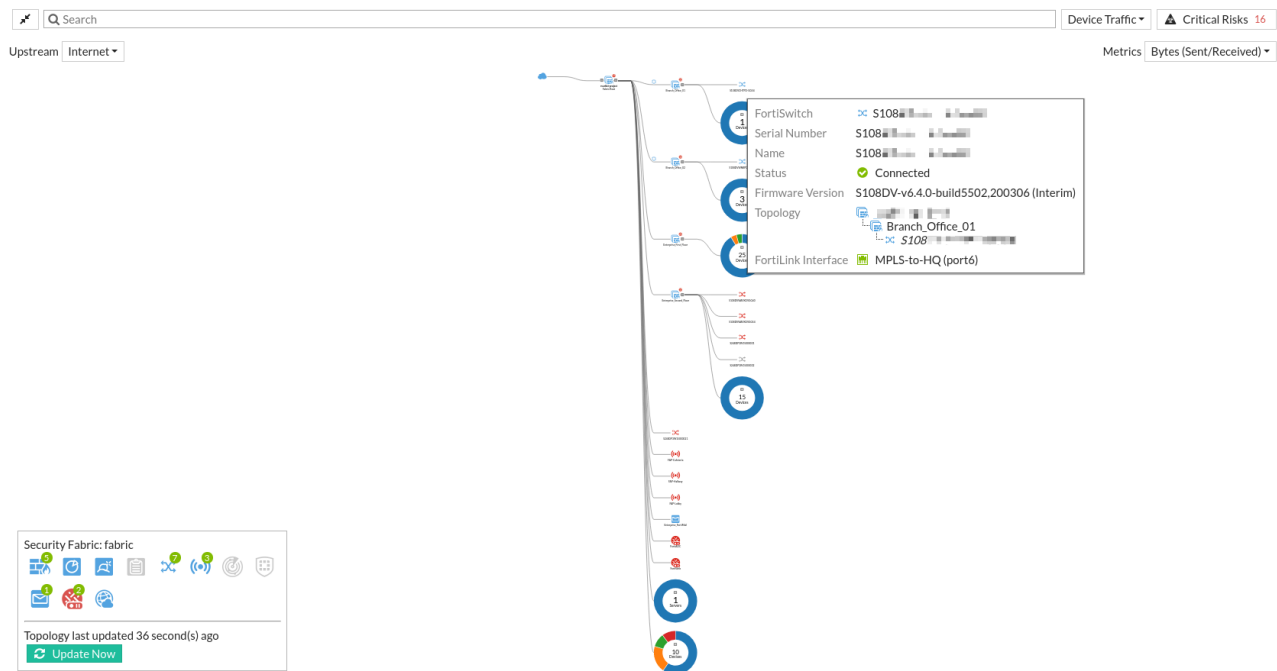
- On the *WiFi & Switch Controller > Managed FortiSwitch* page, the topology view displays FortiSwitches in relation to their own FortiLink stack. In this example, the *newLink* interface currently does not have any FortiSwitches connected to it.



- On the *Security Fabric > Physical Topology* page, hovering over a FortiSwitch displays the *FortiLink Interface* (the



current interface being used by the FortiSwitch).



## Switch controller option to control the sources used to update the user device list - 6.4.2

When the network monitor is enabled on the switch controller, FortiSwitch collects devices information and then populates the FortiGate's device list. You can control the specific sources that are used to populate the device list with the following CLI command:

```
config switch-controller global
    set update-user-device {mac-cache lldp dhcp-snooping l2-db l3-db}
end
```

By default, all of the sources are enabled.

Source	Description
mac-cache	Update MAC addresses from the switch controller mac-cache.
lldp	Update from the FortiSwitch LLDP neighbor database.
dhcp-snooping	Update from the FortiSwitch DHCP snooping client and server databases.
l2-db	Update from the FortiSwitch Network-monitor Layer 2 tracking database.
l3-db	Update from the FortiSwitch Network-monitor Layer 3 tracking database.

For example, to configure FortiSwitch to gather device information through LLDP and the layer 2 and layer 3 tracking databases:

```
config switch-controller global
    set update-user-device lldp l2-db l3-db
end
```

## Log sub-category for switch controller - 6.4.3

FortiSwitch logs now appear as their own subtype (`switch-controller`) in event logs.

To view the FortiSwitch event logs:

1. Go to *Log & Report > Events* and click *FortiSwitch Events*.
2. Double-click an entry to view the log details.

Date/Time	Level	Message	Log Details
2020/08/17 12:16:55	Info	Delete system.sniffer-profile fe:ff:ff:00:00:13	General Date 2020/08/17 Time 12:16:55 Virtual Domain root Log Description FortiSwitch switch
2020/08/17 12:16:55	Info	Delete system.sniffer-profile fe:09:0f:00:0a:01	Source Device ID FGVM02TM20000000 User Fortilink
2020/08/17 12:16:55	Info	Delete system.sniffer-profile 00:03:93:fe:9cd7	Data Message FortiLink: disabled port port1 port-id=1 from b(0) fwd(4)
2020/08/17 12:16:55	Info	Delete system.sniffer-profile 00:03:93:6f:c0fd	Security Level Info
2020/08/17 12:16:55	Info	Delete system.sniffer-profile 00:03:93:8ee3:31	Cellular Serial Number S108DVWA9X000000
2020/08/17 12:16:55	Info	Delete system.sniffer-profile f4:03:04:cb:47:5f	Other ID 6862034115995107416 Time 2020-08-17 12:17:00 euid 3 epid 3 dsteid 3 dstepid 3 logver 604001723 Log ID 0114032697 Type event Sub Type switch-controller Name S108DVWA9X000000 Log event original timestamp 1597691816408384000 Timezone -0700 cd fabric dtime 2020-08-17 12:16:55 itime_t 1597691820 Device Name Enterprise_Second_Floor
2020/08/17 12:16:55	Info	Add system.sniffer-profile fe:ff:ff:00:00:13	
2020/08/17 12:16:55	Info	Add system.sniffer-profile fe:09:0f:00:0a:01	
2020/08/17 12:16:55	Info	Add system.sniffer-profile 00:03:93:fe:9cd7	
2020/08/17 12:16:55	Info	Add system.sniffer-profile 00:03:93:6f:c0fd	
2020/08/17 12:16:55	Info	Add system.sniffer-profile 00:03:93:8ee3:31	
2020/08/17 12:16:55	Info	Add system.sniffer-profile f4:03:04:cb:47:5f	
2020/08/17 12:16:55	Info	Config download successful	
2020/08/17 12:16:55	Info	Edit switch.interface GVM02TM20000000	
2020/08/17 12:16:55	Info	interface internal gets a DHCP lease, ip:169.254.2.2, mask:255.255.255.0, gateway:169.254.2.1	
2020/08/17 12:16:55	Info	Switch-Controller: connected with FortiGate	
2020/08/17 12:16:55	Info	FortiLink: port1 in Fortigate-uplink ready now	
2020/08/17 12:16:55	Info	FortiLink: enable port port1 port-id=1	
2020/08/17 12:16:55	Info	FortiLink: disabled port port1 port-id=1 from b(0) fwd(4)	
2020/08/17 12:16:55	Info	FortiLink: enable port port1 port-id=1	
2020/08/17 12:16:55	Info	primary port GVM02TM20000000 instance 15 changed state from discarding to forwarding	
2020/08/17 12:16:55	Info	primary port GVM02TM20000000 instance 0 changed state from discarding to forwarding	
2020/08/17 12:16:55	Info	FortiLink: port1 joined Fortigate-uplink trunk-id(1)	
2020/08/17 12:16:55	Info	user FortiLink disabled STP on primary interface GVM02TM20000000	
2020/08/17 12:16:55	Info	BPDUGuard: Resetting GVM02TM20000000.	
2020/08/17 12:16:55	Info	primary port GVM02TM20000000 instance 0 changed role from disabled to designated	

To view logs for a specific device:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch* and select a device.
2. Right-click and select *Diagnostics and Tools*.
3. Click the *Logs* tab.

#### 4. Double-click an entry to view the log details.

The screenshot displays the FortiGate web interface. On the left, a sidebar shows a list of devices, with 'S108DVWA9X000000' selected. The main panel shows the 'Diagnostics and Tools' section for this device. It includes a 'General Health' section with metrics like CPU Usage (13%), Memory Usage (24%), Connection Uptime (5 hours), and Temperature. Below this is a 'Faceplate' section with a grid of icons. The 'Logs' tab is selected, showing a table of log entries. The table has columns for Date/Time, Level, Message, and Log Description. The first entry is highlighted, and a 'Log Details' window is open on the right, showing the details of the selected log entry, including Date, Time, Virtual Domain, Log Description, Source (Device ID, User), and Data (Message).

## Configure LLDP settings on a switch port that is leased to a tenant VDOM - 6.4.3

In a tenant VDOM, the LLDP status and profile can be configured on a leased switch port.

In this example, the FortiSwitch and the FortiLink interface are in the `v_home` VDOM. The FortiSwitch's port1 interface is exported to the `v_vip` VDOM, where its LLDP status is set to sending LLDP only and its LLDP profile is set to `voice`.

### To configure port1 in the `v_vip` VDOM:

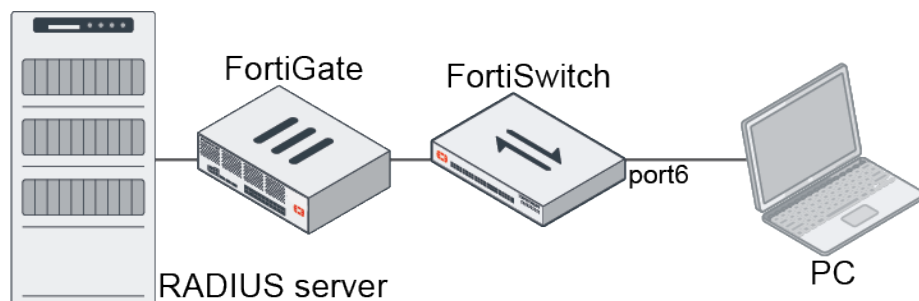
```
config vdom
  edit v_vip
    config switch-controller managed-switch
      edit "S524DN4K15000008"
        set poe-detection-type 3
        set max-allowed-trunk-members 24
        set type virtual
        set owner-vdom "v_home"
      config ports
        edit "port1"
          set vlan "def_vlan_v_vip"
          set lldp-status tx-only
          set lldp-profile "voice"
        next
      end
    next
  end
next
end
```

In the LLDP profile, the automatic inter-switch LAG setting for the tenant port is always disabled, regardless of how it is set in the profile.

## Add a RADIUS timeout VLAN to a security policy - 6.4.3

When an 802.1x authentication request to a RADIUS server times out, the FortiSwitch port can be assigned to the timeout VLAN specified in the security policy.

### Example



In this example, a 802.1x security policy has been applied on port6 of the managed FortiSwitch. The PC tries to authenticate to the RADIUS server, but the server is not available. After 10 seconds, the authentication times out, and the PC is put into the timeout VLAN *vlan22*.

### To configure the security policy:

```

config switch-controller security-policy 802-1X
    edit "auth-timeout"
        set user-group "1X_RADIUS_GROUP"
        set mac-auth-bypass disable
        set open-auth disable
        set eap-passthru enable
        set eap-auto-untagged-vlans enable
        set guest-vlan disable
        set auth-fail-vlan disable
        set framevid-apply enable
        set radius-timeout-overwrite disable
        set authserver-timeout-vlan enable
        set authserver-timeout-period 10
        set authserver-timeout-vlanid "vlan22"
    next
end
  
```

## Add option to enable flow control and pause metering - 6.4.3

Pause metering allows the FortiSwitch to apply flow control to ingress traffic when the queue is congested, and to resume once it is cleared. In FortiOS, flow control and pause metering can be configured in the `switch-controller managed-switch` settings.

Parameter	Description
flow-control {disable   tx   rx   both}	Flow control direction. <ul style="list-style-type: none"> <li>disable: Disable flow control.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>tx: Transmit pause control frames.</li> <li>rx: Receive pause control frames.</li> <li>both: Transmit and receive pause control frames.</li> </ul>
pause-meter <integer>	Ingress metering rate in Kbps (128 – 2147483647, 0 = disable).
pause-meter-resume {75%   50%   25%}	Resume threshold for resuming traffic on the ingress port. The back pressure state will not be cleared until the bucket count falls below 75%, 50%, or 25% of the pause threshold.

### To configure flow control and pause metering:

```
config switch-controller managed-switch
  edit "S248EPTF18000000"
    config ports
      edit "port6"
        set flow-control both
        set pause-meter 2000
        set pause-meter-resume 75%
      next
    end
  next
end
```

## Allow switch controller to set source IP for outbound connections - 6.4.3

By default, a FortiGate uses the outbound interface's IP to communicate with a FortiSwitch managed over layer 3. The `switch-controller-source-ip` option allows the switch controller to use the FortiLink fixed address instead.

Parameter	Description
switch-controller-source-ip	Source IP address for FortiLink traffic. <ul style="list-style-type: none"> <li>outbound: Source IP address is the outbound interface.</li> <li>fixed: Source IP address is the FortiLink interface.</li> </ul>

### To configure the FortiLink interface as the source IP address:

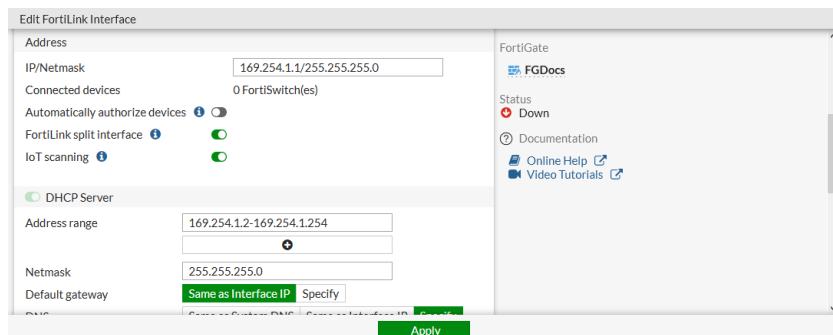
```
config system interface
  edit "fortilink"
    set vdom "vdom1"
    set fortilink enable
    set switch-controller-source-ip fixed
    set ip 169.254.1.1 255.255.255.0
    set allowaccess ping fabric
    set type aggregate
    set member "port7"
    ...
  next
end
```

## Enable IoT background scanning - 6.4.3

Internet of Things (IoT) background scanning is now disabled by default. A valid IoT contract is required to enable it. When IoT scanning is enabled, FortiSwitch will query the FortiGuard IoT service for additional device information.

### To enable IoT background scanning in the GUI:

1. Go to *WiFi & Switch Controller > FortiLink Interface*.
2. Enable *IoT scanning*.



3. Click *Apply*.

### To enable IoT background scanning in the CLI:

```
config system interface
  edit "internal11"
    set vdom "vdom1"
    set fortilink enable
    set ip 169.254.1.1 255.255.255.0
    set allowaccess ping fabric
    set type physical
    set lldp-reception enable
    set lldp-transmission enable
    set snmp-index 11
    set switch-controller-iot-scanning enable
    set lacp-mode static
  next
end
```

## NAC

This section includes information about NAC related new features:

- [Support NAC policies on switch ports on page 465](#)
- [Added ability in FortiSwitch to query FortiGuard IoT service for device details on page 468](#)
- [FortiSwitch voice device detection on page 470](#)
- [Extend NAC matching condition to include EMS tags 6.4.2 on page 474](#)

## Support NAC policies on switch ports

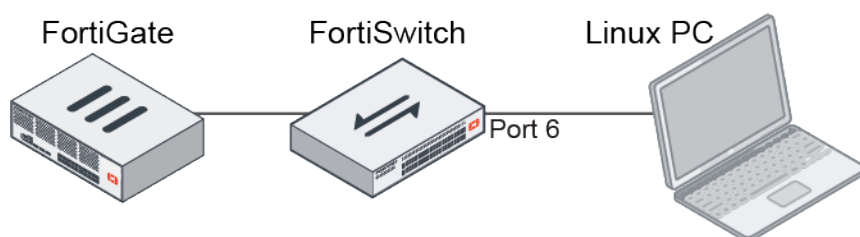
Network access control (NAC) helps administrators implement policies to control the devices and users that have access to their networks. A NAC policy can use user or detected device information, such as device type or OS, to put traffic into a specific VLAN or apply specific port settings.

The NAC function can be enabled on all FortiSwitches, or on specific FortiSwitch ports.

Initially, devices connected to ports with the NAC function enabled are put into an onboarding VLAN. The onboarding VLAN usually has a restrictive security policy, device identification enabled, a DHCP server, and captive portal enabled. The device identification feature collects device information. When the device matches the patterns that are defined in a NAC policy, an action is applied to the device, such as moving it to a specific VLAN or having a security policy applied.

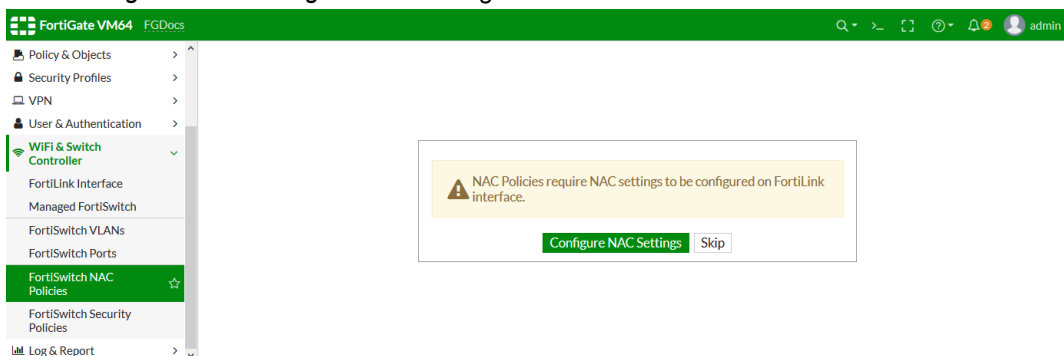
### Example

In this example, NAC settings are enabled and configured so that a Linux PC is automatically moved into a VLAN dedicated to Linux PCs after it comes online and gets identified.

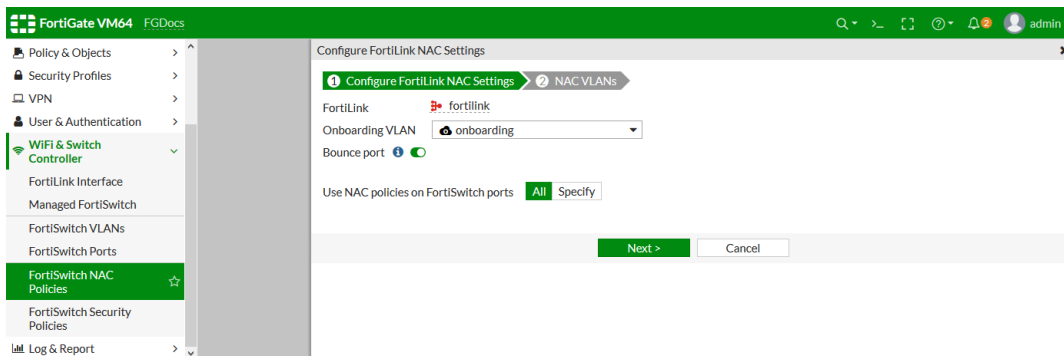


### To configure a NAC policy on a switch in the GUI:

1. Use the wizard to enable the NAC feature and configure basic settings:
  - a. Go to *WiFi & Switch Controller > FortiSwitch NAC Policies*. If FortiSwitch options are not visible, see [Feature visibility](#) for instructions on making them visible.
  - b. Click *Configure NAC Settings* in the message box.

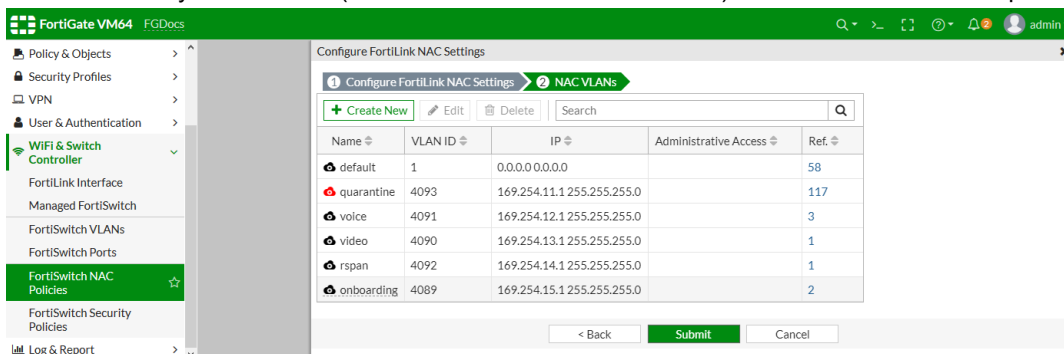


- c. Specify the switch ports that NAC access mode will be enabled on, or enable it on all of them.
- d. Select the onboarding VLAN. If no VLAN exists, click *Create* in the drop down menu to create a new NAC VLAN interface.



e. Click **Next**.

f. Create or modify NAC VLANs (also known as FortiSwitch VLANs) that can be used in NAC policies.



g. Create or edit NAC VLANs as needed. See [FortiLink Setup](#) for details.

h. Click **Submit**.

The NAC settings can be edited in *WiFi & Switch Controller > FortiLink Interface*.

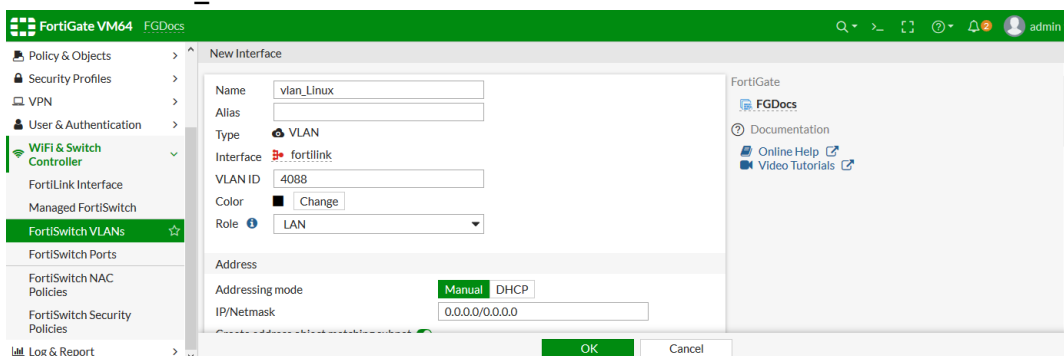
The NAC VLANs can be edited in *WiFi & Switch Controller > FortiSwitch VLANs*.

The access mode of the switch ports is changed to NAC and the native VLAN is set to the onboarding VLAN.

2. Create a NAC VLAN for all Linux PCs:

a. Go to *WiFi & Switch Controller > FortiSwitch VLANs* and click **Create New**.

b. Set **Name** to `vlan_Linux`.



c. Configure the remaining settings as required.

d. Click **OK**.

3. Create a NAC policy to match all Linux PCs and assign them to the specific VLAN:

a. Go to *WiFi & Switch Controller > FortiSwitch NAC Policies* and click **Create New**.

b. Enter a name for the policy, such as `Linux_to_VLAN`.

c. Enable *Operating system* and enter `Linux*` in the field.



- d. Select the *Assign VLAN* card and set VLAN to *vlan\_Linux*.

The screenshot shows the 'Create NAC Policy' window in the FortiGate VM64 GUI. The policy name is 'Linux\_to\_VLAN'. Under 'If device matches all of the following patterns:', the 'Device' category is selected, and the 'Operating system' is set to 'Linux\*'. Under the 'Then:' section, the 'Assign VLAN' option is selected, and the VLAN is set to 'vlan\_Linux'. The 'Traffic action' is set to 'Allow'.

- e. Click OK.

4. After the Linux PC connects, check that it is matched to the policy:

- Go to *WiFi & Switch Controller > FortiSwitch NAC Policies*.
- Select the *Linux\_to\_VLAN* policy and click *View Matched Devices*.

The *Matched Devices* pane opens, showing the devices that matched the policy.

The screenshot shows the 'Matched Devices' pane in the FortiGate VM64 GUI. The table lists devices that matched the 'Linux\_to\_VLAN' policy.

Name	MAC Address	Matched NAC Policy	Assigned VLAN	Status	Last Known Switch	Last Known Port	Description
Linux_to_VLAN	00:0c:29:a9:12:74	Linux_to_Vlan	vlan_Linux	Enable	S124EP5918000276	port6	auto dete

- Go to *WiFi & Switch Controller > FortiSwitch Ports*.

The port that the Linux PC is connected to will include *vlan\_Linux* in the *Allowed VLANs* column.

## To configure a NAC policy on a switch in the CLI:

- Configure the FortiLink interface:

```
config system interface
edit "fortilink"
set vdom "root"
set fortilink enable
set ip 169.254.1.1 255.255.255.0
set allowaccess ping fabric
set type aggregate
set member "internal11"
set lldp-reception enable
set lldp-transmission enable
```

```
        set snmp-index 8
        set auto-auth-extension-device enable
        set switch-controller-nac "fortilink"
    next
end
```

**2. Configure the integrated NAC settings:**

```
config switch-controller nac-settings
    edit "fortilink"
        set mode global
        set onboarding-vlan "onboarding"
    next
end
```

**3. Configure the NAC policy matching pattern to identify matching NAC devices:**

```
config user nac-policy
    edit "Linux_to_VLAN"
        set os "Linux*"
        set switch-fortilink "fortilink"
        set switch-mac-policy "Linux_to_VLAN"
    next
end
```

**4. Configure the MAC policy to be applied on the managed FortiSwitch devices through the NAC device:**

```
config switch-controller mac-policy
    edit "Linux_to_VLAN"
        set fortilink "fortilink"
        set vlan "vlan_Linux"
    next
end
```

**5. View the NAC devices learned on the managed FortiSwitch ports that match the NAC policy:**

```
show switch-controller nac-device
config switch-controller nac-device
    edit 1
        set description "auto detected @ 2020-04-01 15:36:24"
        set mac 00:0c:29:a9:12:74
        set last-known-switch "S124EP5918000276"
        set last-known-port "port6"
        set matched-nac-policy "Linux_to_VLAN"
        set mac-policy "Linux_to_VLAN"
    next
end
```

## Added ability in FortiSwitch to query FortiGuard IoT service for device details

Capability was added to FortiSwitch to work with FortiGate and the new FortiGuard IoT detection service for the purpose of device identification.

FortiSwitch devices are now able to assist FortiGates with capturing the most accurate device information, allowing FortiGate to identify devices for the user device list. When the new FortiGuard IoT detection service is activated, FortiGate will leverage the IoT detection service to help reduce the workload for device identification.



To use this feature, the following are required:

- An IoT detection service subscription. See [IoT detection service on page 258](#).
- FortiSwitch 2.0.3 and higher.

The following CLI command and parameters were added under `switch-controller` to control when FortiSwitch should start and stop collecting device packets for FortiGate:

```
config switch-controller system
  set iot-weight-threshold
  set iot-scan-interval
  set iot-holdoff
  set iot-mac-idle
```

Parameter	Description	Type	Defaults
iot-weight-threshold	The confidence value for the MAC entry. The Value is re-queried when it is below this value.	Integer	<ul style="list-style-type: none"> <li>• Default = 1</li> <li>• Disable = 0</li> </ul>
iot-scan-interval	The IoT scan interval.	Integer	<ul style="list-style-type: none"> <li>• Minimum minutes = 2</li> <li>• Maximum minutes = 4294967295</li> <li>• Default = 60 minutes</li> <li>• Disable = 0</li> </ul>
iot-holdoff	The creation time for the MAC entry. The time must be greater than this value for an entry to be created.	Integer	Default = 5 minutes
iot-mac-idle	The idle time for the MAC entry. The MAC entry is removed after this value.		Default = 1440 minutes

## Example

### Example topology

FGT500E-----FSW248EP(port1)-----FortiAP

In this example, FortiSwitch will help FortiGate collect packets from FortiAP every 30 minutes and stop for 30 minutes. FortiSwitch will stop collecting packets from FortiAP when the weight of the device information reaches a threshold of 80.

### To collect IoT device information for identification in the CLI:

1. This CLI command is configured with the IoT parameters.

```
FGT_A (global) # config switch-controller system
FGT_A (system) # get
```

```

iot-weight-threshold: 80
iot-scan-interval    : 30
iot-holdoff          : 5
iot-mac-idle         : 1440
FGT_A (system) # end

```

2. When the scheduled time to capture the packets is reached, the diagnose command initiates the scan.

```

FGT_A (vdom1) # dia switch-controller traffic-capture show
MAC
=====
name      port      session-in-use  switch      status      fortalink-interface-
=====
08:5b:0e:06:6a:d4      1      S248EPTF18001384      port11
port1      running
Global stats:
=====
node add = 16
node delete = 15
node add failed = 0
node delete failed = 0

```

3. A corresponding sniffer profile is created on FortiSwitch to help collect the data.

```

S524DN4K16000116 # config system sniffer-profile
S524DN4K16000116 (sniffer-profile) # show
config system sniffer-profile
edit "08:5b:0e:06:6a:d4"
set filter "ether host 08:5b:0e:06:6a:d4"
set max-pkt-count 1000
set max-pkt-len 256
set switch-interface "port1"
next
end

```

4. The data is collected and sent to the FortiGuard service for identification. The device information is updated in the device list with *src fortiguard*.

```

FGT_A (vdom1) # dia user device list
hosts
vd vdom1/1 08:5b:0e:06:6a:d4 gen 17 req OUA/34
created 42s gen 13 seen 1s onboarding.13 gen 4
hardware vendor 'FORTINET' src fortiguard id 0 weight 100
type 'Network' src fortiguard id 0 weight 100
family 'Router' src fortiguard id 0 weight 100
os 'NULL' src fortiguard id 0 weight 100
hardware version 'FortiAP-320B' id 0 weight 100
host 'FP320B3X13000599' src capwap

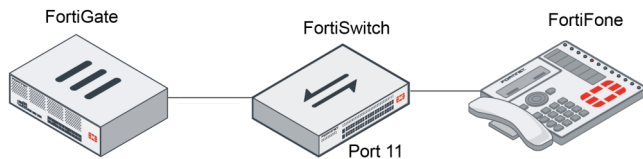
```

## FortiSwitch voice device detection

FortiSwitch is able to parse LLDP messages from voice devices such as FortiFone, and pass this information to FortiGate for device detection. You can use FortiSwitch NAC policies to assign a device to an LLDP profile, QoS policy, and VLAN policy. When a detected device is matched to a NAC policy, the corresponding policy actions will be applied on the switch port.

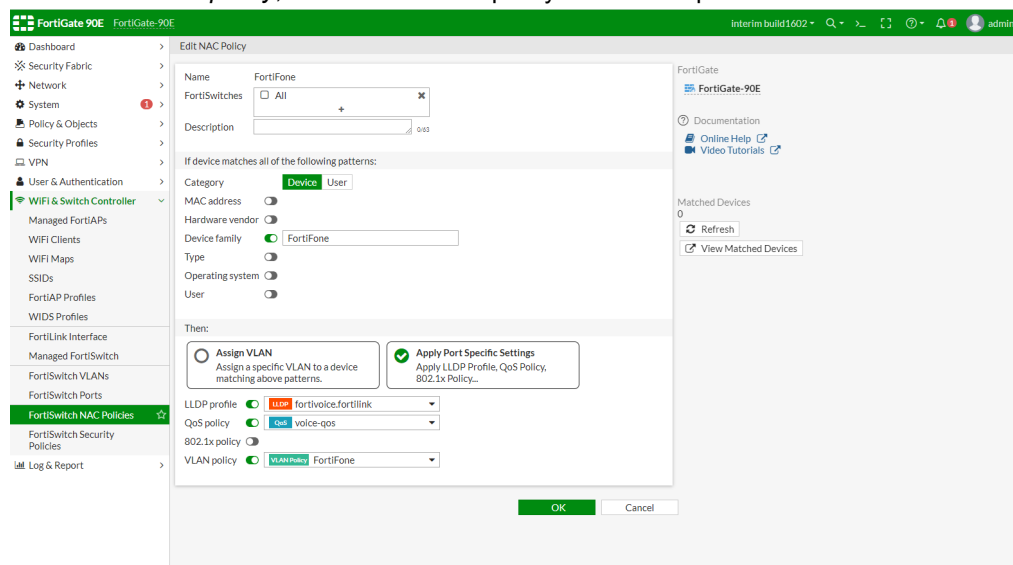
## Example

In the following example, FortiFone is connected to port11 of FortiSwitch. A NAC policy is created to apply a VLAN policy, LLDP policy, and QoS policy to Device Family FortiFone.



### To create a FortiSwitch NAC policy in the GUI:

1. Configure a NAC policy on a switch port. See [Support NAC policies on switch ports on page 465](#).
2. Go to *WiFi & Switch Controller > FortiSwitch NAC Policies*.
3. Create or edit an NAC policy.
4. Configure the NAC policy settings.
  - a. Set the *Category* to *Device*.
  - b. Enable *Device family*, and enter name such as *FortiFone*.
  - c. Select *Apply Port Specific Settings*.
  - d. Enable *LLDP profile*, and select a voice profile from the dropdown.
  - e. Enable *QoS policy*, and select a voice policy from the dropdown.
  - f. Enable *VLAN policy*, and select a voice policy from the dropdown.



The NAC policy is applied after a FortiFone is plugged into port11 of the FortiSwitch:

Port	Trunk	Access Mode	Enabled Features	Native VLAN	Allowed VLANs	LLDP Profile	QoS Policy	Security Policy	Packets (Sent/Re)
port1		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port2		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port3		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port4		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port5		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port6		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		176,924
port7		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port8		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port9		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port10		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port11		NAC	Edge Port Spanning Tree Protocol	voice	quarantine	LLDP fortivoice.fortilink	voice-qos		250,063
port12		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port13		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port14		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0
port15		Normal	Edge Port Spanning Tree Protocol	S524DN4K15000008					853,026
port16		NAC	Edge Port Spanning Tree Protocol	onboarding	quarantine	LLDP default-auto-isl	default		0

## To create a FortiSwitch NAC policy in the CLI:

1. Assign the FortiFone to a VLAN policy, LLDP policy, and QoS Policy.

```

config user nac-policy
edit "FortiFone"
    set family "FortiFone"
    set switch-fortilink "fortilink"
    set switch-port-policy "FortiFone"
next
end

config switch-controller port-policy
edit "FortiFone"
    set fortilink "fortilink"
    set lldp-profile "fortivoice.fortilink"
    set qos-policy "voice-qos"
    set vlan-policy "fortiFone"
next
end

config switch-controller vlan-policy
edit "fortiFone"
    set fortilink "fortilink"
    set vlan "voice"
next
end

config switch-controller lldp-profile
edit "fortivoice.fortilink"
    set med-tlvs inventory-management network-policy location-identification
    set auto-isl disable
    config med-network-policy
        edit "voice"

```

```

        set status enable
        set vlan-intf "voice"
        set assign-vlan enable
        set dscp 46
    next
    edit "voice-signaling"
        set status enable
        set vlan-intf "voice"
        set assign-vlan enable
        set dscp 46
    next
    edit "guest-voice"
    next
    edit "guest-voice-signaling"
    next
    edit "softphone-voice"
    next
    edit "video-conferencing"
    next
    edit "streaming-video"
    next
    edit "video-signaling"
    next
end
next
end

config switch-controller qos qos-policy
    edit "voice-qos"
        set trust-dot1p-map "voice-dot1p"
        set trust-ip-dscp-map "voice-dscp"
        set queue-policy "voice-egress"
    next
end

```

2. FortiSwitch receives an LLDP message from FortiFone after it is plugged into port11.
3. Configure `dia switch-controller switch-info` to check the device information on FortiGate. The FortiFone is identified.

```

FortiGate-90E # dia switch-controller switch-info lldp neighbors-detail
S124EP5918000276 port11

```

Vdom: root

Managed Switch : S124EP5918000276 0

Capability codes:

R:Router, B:Bridge, T:Telephone, C:DOCSIS Cable Device  
W:WLAN Access Point, P:Repeater, S:Station, O:Other

MED TLV Capability codes:

C:Capabilities, P:Network Policies, L:Location, S:MDI PSE  
D:MDI PD, I:Inventory

---

Neighbor learned on port port11 by LLDP protocol

Last change 20 seconds ago

Last packet received 20 seconds ago

Chassis ID: 169.254.15.3 (ip)

```

System Name: FON-675i
System Description:
:14.0.0.1.r4

Time To Live: 60 seconds
System Capabilities: BT
Enabled Capabilities: BT
MED type: Communication Device Endpoint (Class III)
MED Capabilities: CP
Management IP Address: 169.254.15.3

Port ID: 70:4c:a5:e2:6b:b2 (mac)
Port description: WAN Port 10M/100M/1000M
IEEE802.3, Power via MDI:
  Power devicetype: PD
  PSE MDI Power: Not Supported
  PSE MDI Power Enabled: No
  PSE Pair Selection: Can not be controlled
  PSE power pairs: Signal
  Power class: 1 (class-0)
  Power type: 802.3at off
  Power source: Unknown
  Power priority: Unknown
  Power requested: 0.0W
  Power allocated: 0.0W
LLDP-MED, Network Policies:
  voice: VLAN: 256 (untagged), Priority: 0 DSCP: 46
  voice-signaling: VLAN: 256 (untagged), Priority: 0 DSCP: 46
  streaming-video: VLAN: 256 (untagged), Priority: 0 DSCP: 46

FortiGate-90E # dia user device list
hosts
  vd root/0 70:4c:a5:e2:6b:b2 gen 5 req OUA/34
    created 3522s gen 3 seen 24s onboarding gen 2
    hardware vendor 'Fortinet' src lldp weight 128
    type 'IP Phone' src lldp id 1523 weight 128
    family 'FortiFone' src lldp id 1523 weight 128
    host 'FON-675i' src lldp

```

## Extend NAC matching condition to include EMS tags - 6.4.2

The EMS server can now generate a dynamic address with a MAC address. A MAC-based EMS tag can be used as a matching condition in a switch controller NAC policy. The EMS server must be running version 6.4.1 or later.

The following example uses synchronized FortiClient EMS tags from the EMS server. For more information, see [Synchronizing FortiClient EMS tags and configurations](#).

### To use an EMS tag in a NAC policy in the GUI:

1. Go to *WiFi & Switch Controller > FortiSwitch NAC Policies* and click *Create New*.
2. Enter a policy name.
3. For *Category*, select *EMS Tag*.



4. In the *FortiClient EMS Tag* dropdown, select a MAC-based tag.

The screenshot shows the 'Create NAC Policy' configuration window in FortiGate. The 'Name' field is 'nac01', 'Status' is 'Enabled', and 'FortiSwitches' is 'All'. The 'FortiClient EMS Tag' dropdown is open, showing a list of MAC-based tags. The 'Assign VLAN' option is selected under 'Then:'. The 'VLAN' field is empty. The 'OK' button is highlighted in green.

5. Configure the other settings as needed.  
6. Click OK.

### To use an EMS tag in a NAC policy in the CLI:

1. Configure the firewall address:

```
config firewall address
    edit "MAC_FCTEMS0000100000_ems134_vulner_critical_tag"
        set type dynamic
        set sub-type ems-tag
        set comment ''
        set associated-interface ''
        set color 0
        set obj-type mac
    next
end
```

2. Configure the NAC policy:

```
config user nac-policy
    edit "nac01"
        set description ''
        set category ems-tag
        set status enable
        set ems-tag "MAC_FCTEMS0000100000_ems134_win10_tag"
        set switch-fortilink "FortiLink01"
        set switch-auto-auth global
        set switch-port-policy ''
        set switch-mac-policy "nac01"
    next
end
```

## FortiExtender

This section includes information about FortiExtender related new features:

- Support FortiExtender models with two modems 6.4.2 on page 476
- Support data plan profiles for FortiExtender 6.4.2 on page 479

## Support FortiExtender models with two modems - 6.4.2

FortiExtender models such as the FEX-202E and FEX-212E have two modems. Both modems can be configured so virtual interfaces can be associated to them. The following example uses an FEX-212E.

### To configure the FortiExtender in the GUI:

1. Configure the two modems:
  - a. Go to *Network > FortiExtender* and in the top menu, click *Extenders*.
  - b. Double-click the device to edit the settings.
  - c. In the *State* section, ensure the *Authorized* toggle is enabled.
  - d. In the *Modem 1* section, in *Interface* dropdown, click *+ Create*.
  - e. Enter a name and configure the other settings as needed.
  - f. Click *OK*.
  - g. In the *Interface* dropdown, select the newly created interface.
  - h. Repeat these steps for the *Modem 2* section.

The FortiExtender now provides two virtual interfaces (*fext1* and *fext2*) that will be used in the virtual WAN link interface.

The screenshot displays the FortiExtender configuration interface. On the left, the 'Modem 1' section is expanded, showing the 'Interface' dropdown set to 'fext1'. Below this, various settings like 'Default SIM' (SIM1), 'SIM1 PIN', 'SIM2 PIN', 'GPS', 'Auto SIM switch', and 'Switch SIM on disconnect threshold' are visible. The 'Modem 2' section is also expanded, showing its 'Interface' dropdown set to 'fext2'. On the right, a summary panel shows the device model as 'FortiExtender-212E', its connection status as 'Connected', and IP address as '192.168.1.110'. It also displays resource usage for CPU (10%) and Memory (17%), and lists the modem details for both Modem 1 and Modem 2, including their data plans and network types.

2. In the right panel, click *Diagnostics and Tools* to view more details:

a. Click *Modems* to review the modem status.

Diagnostics and Tools - FX212E5919000000

Serial Number	FX212E5919000000
Status	Authorized
Base MAC Address	04d5:90:17:d5:6c
IPv4 Address	192.168.1.110
Version	FXT212E-v4.2-build237
Modem 1 Interface	fext
Modem 2 Interface	fext2

General Health

- CPU Usage: 0%
- Memory Usage: 17%

Modem 1 Health

- Signal Strength: -87 dBm
- Signal Quality: -9.3 dBm

Modem 2 Health

- Signal Strength: -87 dBm
- Signal Quality: -14.8 dBm

Modems SIM Status Diagnostics

	Modem 1	Modem 2
Manufacturer	Sierra Wireless, Incorporated	Sierra Wireless, Incorporated
Assigned Data Plan	Telus-modem1	Fido-modem2
Service	LTE	LTE
Model	EM7565	EM7565

b. Click *SIM Status* to review the SIM status.

Diagnostics and Tools - FX212E5919000000

Serial Number	FX212E5919000000
Status	Authorized
Base MAC Address	04d5:90:17:d5:6c
IPv4 Address	192.168.1.110
Version	FXT212E-v4.2-build237
Modem 1 Interface	fext
Modem 2 Interface	fext2

General Health

- CPU Usage: 0%
- Memory Usage: 17%

Modem 1 Health

- Signal Strength: -87 dBm
- Signal Quality: -9.3 dBm

Modem 2 Health

- Signal Strength: -87 dBm
- Signal Quality: -14.8 dBm

Modems SIM Status Diagnostics

SIM Slot	Status	Carrier	Phone Number	Switch Status	Data Usage	IMSI	IC
<b>Modem 1</b>							
SIM 1	Inserted	Telus	+1-800-387-2222	Active	11 MB of 3000 MB		
SIM 2	Not inserted			Backup	0 MB	N/A	
<b>Modem 2</b>							
SIM 1	Inserted	Generic	+1-800-387-2222	Active	11 MB of 3000 MB		
SIM 2	Not inserted			Backup	0 MB	N/A	

3. Configure the virtual WAN link:

- Go to *Network > SD-WAN Zones* and click *Create New > SD-WAN Member*.
- For *Interface*, select the modem 1 interface (*fext*) and ensure the *Status* is enabled.
- Click *OK*.
- Repeat these steps for the modem 2 interface (*fext2*).

Bandwidth Volume Sessions

Download

Upload

+ Create New Edit Delete

Interfaces	Gateway	Cost	Download	Upload
virtual-wan-link				
fext	10.142.255.141	0	310 bps	119 bps
fext2	25.160.130.72	0	0 bps	0 bps

4. Configure the default static route:

- Go to *Network > Static Routes* and edit the *0.0.0.0/0* route.
- For *Interface*, select *SD-WAN*.
- Ensure the *Status* is enabled.
- Click *OK*.

5. Configure the firewall policy:

- Go to *Policy & Objects > Firewall Policy* and click *Create New*.
- For *Outgoing Interface*, select *virtual-wan-link*.

- c. Configure the other settings as needed.
- d. Click OK.

### To configure the FortiExtender in the CLI:

#### 1. Configure the two modems:

```
config extender-controller extender
  edit "FX212E5919000000"
    set id "FX212E5919000000"
    set authorized enable
    config modem1
      set ifname "fext"
      config auto-switch
        set disconnect enable
        set signal enable
        set dataplan enable
        set switch-back-time "0:1 "
      end
    end
    config modem2
      set ifname "fext2"
      config auto-switch
        set dataplan enable
        set switch-back-time "0:1 "
      end
    end
  end
next
end
```

The FortiExtender now provides two virtual interfaces (`fext` and `fext2`) that will be used in the virtual WAN link interface.

#### 2. Verify the modem settings:

```
get extender modem-status FX212E5919000000 1
Modem 0:
  physical_port:      2-1.2
  manufacture:       Sierra Wireless, Incorporated
  product:            Sierra Wireless, Incorporated
  ....
```

#### 3. Configure the virtual WAN link:

```
config system sdwan
  set status enable
  config zone
    edit "virtual-wan-link"
    next
  end
  config members
    edit 1
      set interface "fext"
    next
    edit 2
      set interface "fext2"
    next
  end
```

```

    end
end

```

#### 4. Configure the default static route:

```

config router static
    edit 2
        set distance 1
        set sdwan enable
    next
end

```

#### 5. Configure the firewall policy:

```

config firewall policy
    edit 1
        set name "fext-traffic"
        set srcintf "wan1"
        set dstintf "virtual-wan-link"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

```

## Support data plan profiles for FortiExtender - 6.4.2

The data plan profile allows users to configure connectivity settings based on modem, carrier, slot, SIM ID, or cost. Users can also specify billing details related to the data plan, as well as smart switch thresholds to define when to switch over to a different SIM.

A FortiExtender has multiple SIM card slots. Certain models also have multiple modems. Essentially, each modem can make one connection with one of the two SIMs associated with the modem. The data plan profile allows users to create general configurations that work across multiple SIMs, or specific profiles that work on a specific SIM. First, the data plan matches the criteria based on the modem ID and type.

### Syntax

```

config extender-controller dataplan
    edit <name>
        set modem-id {modem1 | modem2 | all}
        set type {carrier | slot | iccid | generic}
    end
end

```

Variable	Description
set modem-id ( <i>Available on in the GUI</i> )	Select the match criterion based on the modem: <ul style="list-style-type: none"> <li>modem1: Use modem 1.</li> <li>modem2: Use modem 2.</li> <li>all: Use both modems (default).</li> </ul>
set type ( <i>Type in the GUI</i> )	Select the match criterion based on the type:

Variable	Description
<code>carrier</code> :	Assign by SIM carrier.
<code>slot</code> :	Assign to SIM slot 1 or 2.
<code>iccid</code> :	Assign to a specific SIM by ICCID.
<code>generic</code> :	Compatible with any SIM (default). Assigned if no other data plan matches the chosen SIM.

When a modem connects to the network through a SIM, it will read the SIM information and try to match a data plan based on the modem ID and type. It then uses the data plan connectivity settings to connect (authentication, PDN type, preferred subnet, APN, private network). The billing details (such as the monthly data limit) and smart switch threshold settings define how the SIMs will be switched.

Multiple data plans can be configured:

+ Create New

Edit

Delete

Search

Q

Extenders

Data plans

Name	Modem	Slot/Carrier/ICCID	APN	Capacity	Monthly Cost	Billing Date
Carrier						
Bell		Bell		6000	0	
Fido-modem2		Generic		3000	0	
Telus-modem1		Telus		2000	0	

Once the FortiExtender is controlled by the FortiGate, the data plan is sent to the FortiExtender. The format is identical between devices.

### To configure a data plan in the GUI:

1. Go to *Network > FortiExtender* and in the top menu, click *Data plans*.
2. Click *Create New*.
3. Enter a name and ensure the *Status* is enabled.
4. For *Available on*, select a criterion (*Modem 1*, *Modem 2*, or *All Modems*).
5. For *Type* select a criterion (*Carrier*, *ATCA Slot*, *ICCID*, or *generic*).
6. Configure the other settings as needed (*Connectivity*, *Billing Details*, and *Smart Switch threshold*).

7. Click *OK*.

**To configure a data plan in the CLI:**

```
config extender-controller dataplan
  edit "Telus-modem1"
    set modem-id modem1
    set type carrier
    set carrier "Telus"
    set capacity 2000
    set billing-date 30
  next
  edit "Fido-modem2"
    set modem-id modem2
    set type carrier
    set carrier "Generic"
    set capacity 3000
  next
  edit "Bell"
    set type carrier
    set carrier "Bell"
    set APN "pda.bell.ca"
    set capacity 6000
  next
end
```

# Log and report

This section includes information about logging and reporting related new features:

- [Logging on page 482](#)

## Logging

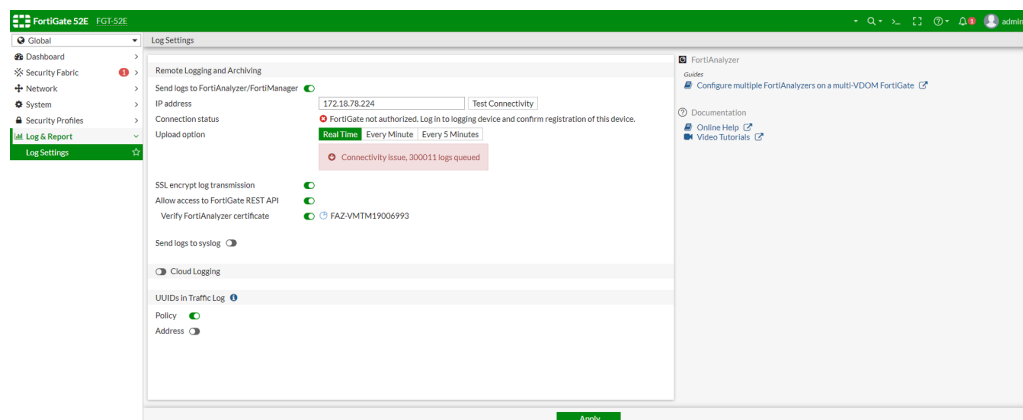
This section includes information about logging related new features:

- [Log buffer on FortiGates with an SSD disk on page 482](#)
- [WAD and Proxyd SSL logging improvement on page 485](#)
- [WAN interface bandwidth log on page 489](#)
- [Include RSSO information for authenticated destination users in logs 6.4.1 on page 491](#)
- [Application logging in NGFW policy mode 6.4.2 on page 494](#)
- [Send traffic logs to FortiAnalyzer Cloud 6.4.4 on page 495](#)
- [Log updates to dynamic objects 6.4.5 on page 498](#)

## Log buffer on FortiGates with an SSD disk

FortiGates with an SSD disk have a configurable log buffer. When the connection to FortiAnalyzer is unreachable, the FortiGate is able to buffer logs on disk if the memory log buffer is full. The logs queued on the disk buffer can be sent successfully once the connection to FortiAnalyzer is restored.

The number of logs queued on the disk buffer is visible in the *Log & Report > Log Settings* page:



The queued logs are buffered to the memory first and then disk. Main `miglogd` handles the disk buffering job, while `miglogd-children` handles the memory buffering. Disk buffer statistics only appear under Main `miglogd`, and memory buffer statistics only appears under `miglogd-children`. If the total buffer is full, new logs will overwrite the old logs.



**To configure the log buffer:**

1. Allocate disk space (MB) to temporarily store logs to FortiAnalyzer:

```
config system global
    set faz-disk-buffer-size 200
end
```

2. Check the Main `miglogd` and `miglogd-children` statistics. The 200 MB disk buffer has been set, and there are currently no logs buffered in memory or on disk when FortiAnalyzer is reachable:

```
# diagnose test application miglogd 41 0
cache maximum: 106100940(101MB) objects: 0 used: 0(0MB) allocated: 0(0MB)
VDOM:root
Queue for: global-faz
```

```
memory queue:
    num:0 size:0(0MB) max:101906636(97MB) logs:0
```

```
disk max queue size:200MB total:0MB
total items:0
disk queue agents:
    devid:-1-10-0-1
    buffer path:/var/log/qbuf/10.0/1
    saved size:0MB cached size:0
    save roll:0 restore roll:0
    restore id:0 space:0MB
```

```
# diagnose test application miglogd 41 1
cache maximum: 106100940(101MB) objects: 0 used: 0(0MB) allocated: 0(0MB)
VDOM:root
Queue for: global-faz
```

```
memory queue:
    num:0 size:0(0MB) max:101906636(97MB) logs:0
```

```
disk queue client:
    devid:-1-10-0-1 status:buffering
    Total in cache:0 size:0(0MB) max:4MB logs:0
```

3. Disable the connection between the FortiGate and FortiAnalyzer. For example, delete the FortiGate from the FortiAnalyzer authorized device list.

Assuming a massive number of logs (~ 300000) are recorded during this downtime, the logs will be queued in the memory buffer first. If the memory buffer is full, then the remaining logs will be queued on the disk buffer.

4. Check the Main `miglogd` and `miglogd-children` statistics again. All 97 MB of the memory buffer is occupied, and 76 of the 200 MB has been taken from the disk buffer:

```
# diagnose test application miglogd 41 0
cache maximum: 106100940(101MB) objects: 0 used: 0(0MB) allocated: 0(0MB)
VDOM:root
Queue for: global-faz
```

```
memory queue:
    num:0 size:0(0MB) max:101906636(97MB) logs:0
```

```
disk max queue size:200MB total:76MB
total items:128917
```

```

disk queue agents:
    devid:-1-10-0-1
    buffer path:/var/log/qbuf/10.0/1
    saved size:76MB cached size:3324984
    save roll:19 restore roll:0
    restore id:0 space:0MB

# diagnose test application miglogd 41 1
cache maximum: 106100940(101MB) objects: 165721 used: 101908358(97MB) allocated:
106449280(101MB)
VDOM:root
Queue for: global-faz

```

```

memory queue:
    num:165718 size:101906500(97MB) max:101906636(97MB) logs:165718

```

```

disk queue client:
    devid:-1-10-0-1 status:restoring
    restore id:1267 space:0MB
    Total in cache:3 size:1858(0MB) max:4MB logs:3

```

The overall miglogd statistics shows the total cached logs is the sum of the logs buffered in memory and on disk:

```

# diagnose test application miglogd 6
mem=0, disk=11, alert=0, alarm=0, sys=0, faz=300053, faz-cloud=0, webt=0, fds=0
interface-missed=44
Queues in all miglogds: cur:165718 total-so-far:165718
global log dev statistics:
faz 0: sent=0, failed=0, cached=300053, dropped=0 , relayed=0
Num of REST URLs: 0

```

5. Enable the connection between FortiAnalyzer and the FortiGate.
6. After a while, check the miglogd statistics to confirm that all buffered logs are being sent to FortiAnalyzer successfully:

```

# diagnose test application miglogd 6
mem=0, disk=11, alert=0, alarm=0, sys=0, faz=300058, faz-cloud=0, webt=0, fds=0
interface-missed=44
Queues in all miglogds: cur:4294832957 total-so-far:165726
global log dev statistics:
faz 0: sent=300058, failed=0, cached=0, dropped=0 , relayed=0
Num of REST URLs: 15

```

```

# diagnose test application miglogd 41 0
cache maximum: 106100940(101MB) objects: 0 used: 0(0MB) allocated: 0(0MB)
VDOM:root
Queue for: global-faz

```

```

memory queue:
    num:0 size:0(0MB) max:101906636(97MB) logs:0

```

```

disk max queue size:200MB total:0MB
total items:0
disk queue agents:
    devid:-1-10-0-1
    buffer path:/var/log/qbuf/10.0/1
    saved size:0MB cached size:0

```

```

save roll:20 restore roll:20
restore id:1267 space:0MB

# diagnose test application miglogd 41 1
cache maximum: 106100940(101MB) objects: 0 used: 0(0MB) allocated: 0(0MB)
VDOM:root
Queue for: global-faz

memory queue:
    num:0 size:0(0MB) max:101906636(97MB) logs:0

disk queue client:
    devid:-1-10-0-1 status:buffering
    Total in cache:0 size:0(0MB) max:4MB logs:0

```

## WAD and Proxyd SSL logging improvement

During deep inspection and certificate inspection, various logs generated from certificate issues now use a consistent log format. Additional details have also been added to these logs. A new option, `ssl-negotiation-log`, captures results of unsupported SSL negotiations.

### SSL/SSH protocol options:

A new option, `set ssl-negotiation-log {enable | disable}`, was added to the option set.

```

config firewall ssl-ssh-profile
edit "deep-inspection"
    set ssl-anomalies-log {enable | disable}
    set ssl-exemptions-log {enable | disable}
    set ssl-negotiation-log {enable | disable}
next
end

```

### To log invalid certificates:

```

config firewall ssl-ssh-profile
edit "deep-inspection"
    set ssl-anomalies-log enable
next
end

```

FortiGate will generate the ssl anomalies log when traffic triggers ssl certificate anomalies.

In the HTTPS and SMTPS version of the traffic and ssl utm logs:

- The `logid` and the server certificate CN are the same.
- The `msg` field in the SSL UTM logs are similar.

Log type	HTTP	SMTPS
Traffic log	1: date=2020-02-06 time=10:54:36 logid="0000000013" type="traffic"	6: date=2020-02-06 time=11:02:57 logid="0000000013" type="traffic"

Log type	HTTP	SMTPS
	<pre> subtype="forward" level="notice" vd="vdom1" eventtime=1581015276280004271 tz="-0800" srcip=10.1.100.66 srcport=45068 srcintf="port2" srcintfrole="undefined" dstip=172.16.200.99 dstport=443 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=95917 proto=6 action="server-rst" policyid=1 policytype="policy" poluuid="81d655f2-479f-51ea-d1d1-5fd661144c81" service="HTTPS" trandisp="snat" transip=172.16.200.7 transport=45068 duration=5 sentbyte=931 rcvbyte=6818 sentpkt=11 rcvpkt=11 appcat="unscanned" wanin=0 wanout=0 lanin=696 lanout=696 utmaction="block" countssl=1 crscore=5 craction=262144 crlevel="low" utmref=65503-98 </pre>	<pre> subtype="forward" level="notice" vd="vdom1" eventtime=1581015777090002933 tz="-0800" srcip=10.1.100.66 srcport=57522 srcintf="port2" srcintfrole="undefined" dstip=172.16.200.99 dstport=465 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=96269 proto=6 action="close" policyid=1 policytype="policy" poluuid="81d655f2-479f-51ea-d1d1-5fd661144c81" service="SMTPS" trandisp="snat" transip=172.16.200.7 transport=57522 duration=5 sentbyte=597 rcvbyte=216 sentpkt=6 rcvpkt=4 appcat="unscanned" utmaction="block" countssl=1 utmref=65500-0 </pre>
<b>SSL UTM log</b>	<pre> 1: date=2020-02-06 time=10:54:31 <b>logid="1700062303"</b> type="utm" subtype="ssl" <b>eventtype="ssl-anomalies"</b> level="warning" vd="vdom1" eventtime=1581015271212451397 tz="-0800" action="blocked" policyid=1 sessionid=95917 service="HTTPS" profile="deep-inspection-clone" srcip=10.1.100.66 srcport=45068 dstip=172.16.200.99 dstport=443 srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6 eventsubtype="certificate-anomaly" <b>msg="SSL connection is blocked, certificate-status: expired."</b> <b>hostname="invalid.fortinet.com"</b> </pre>	<pre> 1: date=2020-02-06 time=11:02:52 <b>logid="1700062303"</b> type="utm" subtype="ssl" <b>eventtype="ssl-anomalies"</b> level="warning" vd="vdom1" eventtime=1581015771995913532 tz="-0800" action="blocked" policyid=1 sessionid=96269 service="SMTPS" profile="deep-inspection-clone" srcip=10.1.100.66 srcport=57522 dstip=172.16.200.99 dstport=465 srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6 eventsubtype="certificate-anomaly" <b>msg="SSL connection is blocked, certificate-status: expired untrusted validation_failure."</b> <b>hostname="invalid.fortinet.com"</b> </pre>

### To log SSL Exemptions based on FortiGuard categories:

```

config firewall ssl-ssh-profile
edit "deep-inspection-clone"

```

```

set ssl-exemptions-log enable
next
end

```

In the HTTPS and SMTPS version of the traffic and ssl utm logs:

- The `logid` and the `msg` are the same.
- A server certificate CN is added to the log.



FortiGate records the wrong category ID and description in the HTTPS version of the ssl utm log. This is a known issue.

Log type	HTTPS	SMTPS
<b>Traffic log</b>	<pre> 8: date=2020-02-06 time=15:46:10 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vdom1" eventtime=1581032769970002679 tz="-0800" srcip=10.1.100.66 srcport=57116 srcintf="port2" srcintfrole="undefined" dstip=52.52.208.2 dstport=443 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="United States" sessionid=107685 proto=6 action="close" policyid=1 policytype="policy" poluid="81d655f2-479f-51ea-d1d1-5fd661144c81" service="HTTPS" trandisp="snat" transip=172.16.200.7 transport=57116 duration=1 sentbyte=1925 rcvdbyte=7736 sentpkt=13 rcvdpkt=13 appcat="unscanned" wanin=0 wanout=0 lanin=1241 lanout=1241 utmaction="allow" countssl=1 utmref=65476-42 </pre>	<pre> 1: date=2020-02-07 time=10:39:20 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vdom1" eventtime=1581100760770003429 tz="-0800" srcip=10.1.100.66 srcport=42638 srcintf="port2" srcintfrole="undefined" dstip=74.125.195.109 dstport=465 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="United States" sessionid=139840 proto=6 action="close" policyid=1 policytype="policy" poluid="81d655f2-479f-51ea-d1d1-5fd661144c81" service="SMTPS" trandisp="snat" transip=172.16.200.7 transport=42638 duration=1 sentbyte=896 rcvdbyte=3392 sentpkt=9 rcvdpkt=7 appcat="unscanned" utmaction="allow" countssl=1 utmref=65470-0 </pre>
<b>SSL UTM log</b>	<pre> 1: date=2020-02-06 time=15:46:08 logid="1701062005" type="utm" subtype="ssl" eventtype="ssl-exempt" level="notice" vd="vdom1" eventtime=1581032768540281919 tz="-0800" action="exempt" policyid=1 sessionid=107685 service="HTTPS" </pre>	<pre> 1: date=2020-02-07 time=10:39:19 logid="1701062005" type="utm" subtype="ssl" eventtype="ssl-exempt" level="notice" vd="vdom1" eventtime=1581100759642872145 tz="-0800" action="exempt" policyid=1 sessionid=139840 service="SMTPS" </pre>

Log type	HTTPS	SMTPS
	<pre> profile="deep-inspection-clone" srcip=10.1.100.66 srcport=57116 dstip=52.52.208.2 dstport=443 srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6 eventsubtype="fortiguard-category" cat=1 catdesc="Drug Abuse" hostname="www.fortinet.com" msg="SSL connection is exempted based on category rating." </pre>	<pre> profile="deep-inspection-clone" srcip=10.1.100.66 srcport=42638 dstip=74.125.195.109 dstport=465 srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6 eventsubtype="fortiguard-category" cat=23 catdesc="Web-based Email" hostname="smtp.gmail.com" msg="SSL connection is exempted based on category rating." </pre>

### To log unsupported SSL negotiation:

```

config firewall ssl-ssh-profile
  edit "deep-inspection-clone"
    set ssl-negotiation-log enable
  next
end

```

The `logid` and `msg` fields are the same in the HTTPS and IMAPS version of the traffic and ssl utm logs:

Log type	HTTPS	IMAPS
<b>Traffic log</b>	<pre> 1: date=2020-02-07 time=11:10:59 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vdom1" eventtime=1581102659640002285 tz="-0800" srcip=10.1.100.66 srcport=33666 srcintf="port2" srcintfrole="undefined" dstip=172.16.200.99 dstport=8080 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=141224 proto=6 action="close" policyid=1 policytype="policy" poluuid="81d655f2-479f-51ea-d1d1-5fd661144c81" service="tcp/8080" trandisp="snat" transip=172.16.200.7 transport=33666 duration=1 sentbyte=216 rcvdbyte=216 sentpkt=4 rcvdpkt=4 appcat="unscanned" wanin=0 </pre>	<pre> 16: date=2020-02-07 time=11:06:55 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vdom1" eventtime=1581102415810001699 tz="-0800" srcip=10.1.100.66 srcport=58162 srcintf="port2" srcintfrole="undefined" dstip=172.16.200.99 dstport=8143 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=141051 proto=6 action="close" policyid=1 policytype="policy" poluuid="81d655f2-479f-51ea-d1d1-5fd661144c81" service="tcp/8143" trandisp="snat" transip=172.16.200.7 transport=58162 duration=5 sentbyte=216 rcvdbyte=164 sentpkt=4 rcvdpkt=3 appcat="unscanned" </pre>

Log type	HTTPS	IMAPS
	wanout=0 lanin=82 lanout=82 utmaction="block" countssl=1 utmref=65464-0	utmaction="block" countssl=1 utmref=65467-0
<b>SSL UTM log</b>	1: date=2020-02-07 time=11:10:58 <b>logid="1702062101"</b> type="utm" subtype="ssl" <b>eventtype="ssl-negotiation"</b> level="warning" vd="vdom1" eventtime=1581102658589415731 tz="-0800" action="blocked" policyid=1 sessionid=141224 service="HTTPS" profile="deep-inspection-clone" srcip=10.1.100.66 srcport=33666 dstip=172.16.200.99 dstport=8080 srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6 <b>eventsubtype="unexpected-protocol"</b> <b>msg="SSL connection is blocked."</b>	1: date=2020-02-07 time=11:06:50 <b>logid="1702062101"</b> type="utm" subtype="ssl" <b>eventtype="ssl-negotiation"</b> level="warning" vd="vdom1" eventtime=1581102410702684472 tz="-0800" action="blocked" policyid=1 sessionid=141051 service="IMAPS" profile="deep-inspection-clone" srcip=10.1.100.66 srcport=58162 dstip=172.16.200.99 dstport=8143 srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6 <b>eventsubtype="unexpected-protocol"</b> <b>msg="SSL connection is blocked."</b>

## WAN interface bandwidth log

In the system performance statistics event log, `waninfo` (logID 40704) collects WAN interface information for analyzing purpose by FortiAnalyzer. The log supports up to three interfaces assigned a WAN role and the interfaces are displayed in alphabetical order.

### To view the WAN interface bandwidth log in the GUI:

1. Go to *Log & Report > Events*.
2. On the toolbar menu, select the *System Events* subtype from the dropdown.
3. Select a *Performance statistics* log.

#### 4. Click *Details* and scroll to view the *WAN Interface Information* (log ID 40704).

#### To view the WAN interface bandwidth log in the CLI:

```
# execute log filter device fortianalyzer
# execute log filter category event
# execute log filter action "perf-stats"
# execute log display
```

#### Sample logs

When no WAN interface role is configured:

```
1: date=2020-01-24 time=11:17:57 logid="0100040704" type="event" subtype="system"
level="notice" vd="vdom1" eventtime=1579893477525796593 tz="-0800" logdesc="System
performance statistics" action="perf-stats" cpu=0 mem=19 totalsession=26 disk=1
bandwidth="46/127" setuprate=0 disklograte=0 fazlograte=0 freediskstorage=28349
sysuptime=4869 waninfo="N/A" msg="Performance statistics: average CPU: 0, memory: 19,
concurrent sessions: 26, setup-rate: 0"
```

After three WAN interface roles are configured:

```
1: date=2020-01-24 time=11:26:58 logid="0100040704" type="event" subtype="system"
level="notice" vd="vdom1" eventtime=1579894018320178732 tz="-0800" logdesc="System
performance statistics" action="perf-stats" cpu=0 mem=19 totalsession=38 disk=1
bandwidth="40/95" setuprate=0 disklograte=0 fazlograte=0 freediskstorage=28349
sysuptime=5410
waninfo="name=dmz,bytes=6519/294381,packets=50/2407;name=ha1,bytes=474/0,packets=5/0;name=wa
n1,bytes=92312156/46493734,packets=811589/362592;" msg="Performance statistics: average CPU:
0, memory: 19, concurrent sessions: 38, setup-rate: 0"
```

After four WAN interface roles are configured:

```
1: date=2020-01-24 time=15:25:45 logid="0100040704" type="event" subtype="system"
level="notice" vd="root" eventtime=1579908345124515733 tz="-0800" logdesc="System
performance statistics" action="perf-stats" cpu=1 mem=34 totalsession=14 disk=1
bandwidth="120/93" setuprate=0 disklograte=0 fazlograte=0 freediskstorage=113870
sysuptime=603047
```



```
waninfo="name=~@.TEST.....,bytes=16878/1057173,packets=282/3200;name=port2,bytes=178589214/140899648,packets=657920/769158;name=wan1,bytes=90/184,packets=1/2;" msg="Performance statistics: average CPU: 1, memory: 34, concurrent sessions: 14, setup-rate: 0"
```

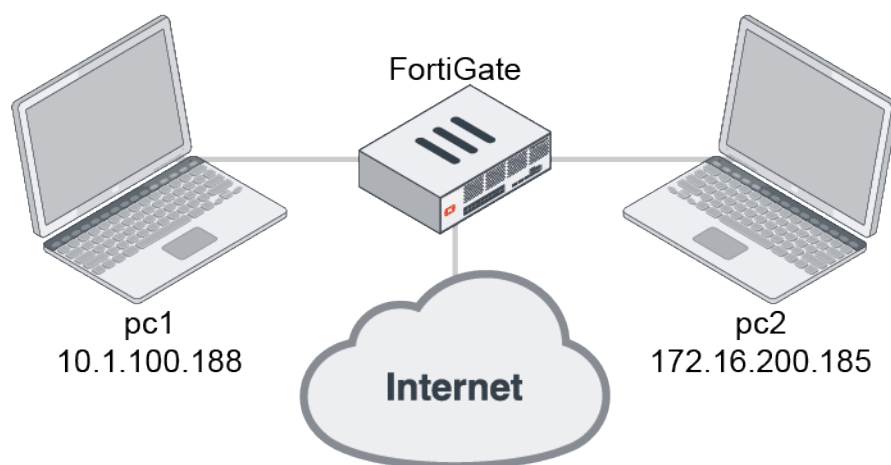
## Include RSSO information for authenticated destination users in logs - 6.4.1

FortiGate can now use RSSO accounting information from authenticated RSSO users to populate destination users and groups, along with source users and groups.

RSSO user login information can be forwarded by the RADIUS server to the FortiGate that is listening for incoming RADIUS accounting start messages on the RADIUS accounting port. Accounting start messages usually contain the IP address, user name, and user group information. FortiGate uses this information in traffic logs, which now include *dstuser* and *dstgroup* fields for user and group destination information.

For instructions on configuring RSSO, see [RADIUS single sign-on agent](#).

The three following scenarios show traffic between pc1 and the internet, and pc1 and pc2.



### Scenario 1

In this scenario, RSSO user *test2* in group *rsso-grp1* is authenticated on pc1. Traffic flows from pc1 to the internet.

#### Expected result:

In the logs, user *test2* is shown as the source user in the *rsso-grp1* group.

**To verify the results:**

1. In the GUI, go to *Log & Report > Forward Traffic* and view the details of an entry with test2 as the source.
2. In the *Source* section, *User* is *test2* and *Group* is the *rsso-grp1*.

Date/Time	Source	Device	Destination	Application Name	Result
2020/05/26 14:37:33	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	52.38.8.230		
2020/05/26 14:37:29	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	54.153.103.110 (ups.analytics.yahoo.com)		
2020/05/26 14:37:26	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	172.217.14.226 (www.googleadservices.com)		
2020/05/26 14:37:25	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	216.58.217.35 (ssl.gstatic.com)		
2020/05/26 14:37:23	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	23.111.11.182 (a.opnmstr.com)		2.54 MB / 713
2020/05/26 14:37:22	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	172.217.3.195 (fonts.gstatic.com)		1.00 MB / 4.17
2020/05/26 14:37:13	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	172.16.200.131		14.79 MB / 26
2020/05/26 14:37:09	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	10.6.30.16		256 B / 224 B
2020/05/26 14:37:09	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	10.6.30.16		256 B / 224 B
2020/05/26 14:37:09	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	10.6.30.16		256 B / 224 B
2020/05/26 14:36:47	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	10.6.30.134		104.63 KB / 2
2020/05/26 14:36:43	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	10.6.30.131		132.01 MB / 3
2020/05/26 14:36:33	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	10.6.30.16		
2020/05/26 14:36:16	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	172.16.200.142		3.42 MB / 1.96
2020/05/26 14:36:06	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	172.16.200.142		
2020/05/26 14:36:06	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	20.189.79.72		76 B / 76 B
2020/05/26 14:36:50	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	172.16.200.194		11.73 MB / 22
2020/05/26 14:36:18	10.1.100.210	GENERIC/PPPO	10.6.30.201		84 B / 84 B
2020/05/26 14:36:13	10.1.100.251	win2012-fsso-3.Fortinet-FSSO.COM	172.16.200.131		14.73 MB / 26
2020/05/26 14:34:59	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	172.16.200.185		290 B / 508 B
2020/05/26 14:34:58	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	172.16.200.185		290 B / 508 B
2020/05/26 14:34:58	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	172.16.200.185		290 B / 508 B
2020/05/26 14:34:57	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	172.16.200.185		290 B / 508 B
2020/05/26 14:34:55	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	172.16.200.185		290 B / 508 B
2020/05/26 14:34:54	test2 (10.1.100.188)	win7-2-A.Fortinet-FSSO.COM	172.16.200.185		290 B / 508 B

**Log Details**  
**General**  
Date: 2020/05/26  
Time: 14:37:33  
Duration: 14s  
Session ID: 48958  
Virtual Domain: vdom1  
NAT Translation: Source  
**Source**  
IP: 10.1.100.188  
NAT IP: 172.16.200.1  
Source Port: 49891  
Country/Region: Reserved  
Primary MAC: 00:0c:29:44:be:b9  
Source Interface: port10  
Source Host Name: win7-2-A.Fortinet-FSSO.COM  
OS Name: Windows  
User: test2  
Group: rsso-grp1  
**Destination**  
IP: 52.38.8.230  
Port: 443  
Country/Region: United States  
Destination Interface: port9  
**Application Control**  
Application Name:  
Category: unscanned  
Risk: undefined  
Protocol: 8  
Service: HTTPS  
**Data**  
Received Bytes: 5 KB  
Sent Bytes: 3 KB  
Sent Packets: 16  
**Action**  
Action: TCP reset from client  
Reason: null / 1%

3. The log message shows the user and group:

```
10: date=2020-05-25 time=15:34:43 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1590446083718007055 tz="-0700" srcip=10.1.100.188
srcname="win7-2-A.Fortinet-FSSO.COM" srcport=56982 srcintf="port10"
srcintfrole="undefined" dstip=172.217.3.195 dstport=443 dstintf="port9"
dstintfrole="undefined" srccountry="Reserved" dstcountry="United States"
sessionid=120651 proto=17 action="accept" policyid=1 policytype="policy"
poluid="d130f886-9ec6-51ea-206e-8c561c5244c6" policyname="pol1" user="test2"
group="rsso-grp1" authserver="vdom1" service="udp/443"trandisp="snat"
transip=172.16.200.1 transport=56982 duration=181 sentbyte=2001 rcvdbyte=1820 sentpkt=6
rcvdpkt=4 appcat="unscanned" sentdelta=0 rcvddelta=0 srchwvender="VMware"
osname="Windows" srcswversion="7" mastersrcmac="00:0c:29:44:be:b9"
srcmac="00:0c:29:44:be:b9" srcserver=0
```

**Scenario 2**

In this scenario, RSSO user *test2* is authenticated on pc1. Traffic is initialized on pc2 (172.16.200.185) going to pc1 (10.1.100.188).

**Expected result:**

In the logs, user *test2* is shown as the destination user (*dstuser*). No destination group (*dstgroup*) is logged because no RSSO user is logged in on pc2, so the traffic from pc2 is unauthenticated.

**To verify the results:**

1. In the GUI, go to *Log & Report > Forward Traffic* and view the details of an entry with 172.16.200.185 (pc2) as the source.

2. In the *Other* section, *Destination User* is *test2* and no destination group is shown.

DateTime	Source	Device	Destination	Application N.	Result	Policy ID	Log Details
20200526 14:56:55	test2 (10.1.100.180)	win7-2-A.Fortinet.F880.COM	99.86.38.97 (embeds.driftn.com)		port (1)		<b>Destination</b> IP 10.1.100.180 Port 80 Destination MAC 00:0c:29:44:be:b9 Country/Region Reserved Destination Interface port0
20200526 14:56:44	172.16.200.185		10.1.100.188		✓ 328 B / 563 B	pol2 (2)	<b>Application Control</b> Application Name Category unscanned Risk undefined Protocol 6 Service HTTP
20200526 14:56:43	172.16.200.185		10.1.100.188		✓ 328 B / 563 B	pol2 (2)	<b>Data</b> Received Bytes 563 B Received Packets 5 Sent Bytes 328 B Sent Packets 6
20200526 14:56:42	172.16.200.185		10.1.100.188		✓ 328 B / 563 B	pol2 (2)	<b>Action</b> Action Accept session close Policy ID pol2 (2) Policy 2894368:Seca-Step-04c UUID ec5a6c1d5943 Policy Type Forward
20200526 14:56:38	172.16.200.185		10.1.100.188		✓ 328 B / 563 B	pol2 (2)	<b>Security</b> Level [     ]
20200526 14:56:37	172.16.200.185		10.1.100.188		✓ 328 B / 563 B	pol2 (2)	<b>Cellular</b> Service HTTP
							<b>Other</b> Log ID 0000000013 Type traffic Sub Type forward Log event original 1600530197271602500 Timestamp -0700 Source Interface Role undefined Destination Interface Role undefined Policy Name pol2 Destination User test2 Destination Authentication Server upm1 Destination Hardware Vendor VMware Destination OS Name Windows Destination Software Version 7

3. The log message shows the destination user:

```
1: date=2020-05-22 time=07:38:06 logid="0000000020" type="traffic" subtype="forward"
level="notice" vd="root" eventtime=1590158286585506922 tz="-0700" srcip=172.16.200.185
identifier=1 srcintf="port9" srcintfrole="undefined" dstip=10.1.100.188 dstintf="port10"
dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=4395
proto=1 action="accept" policyid=3 policytype="policy" poluuid="d4f18e1e-9c36-51ea-6ec0-
3a354d5910ee" policyname="pol2" dstuser="test2" dstauthserver="root" service="PING"
trandisp="snat" transip=10.1.100.1 transport=0 duration=128 sentbyte=7620 rcvdbyte=5220
sentpkt=127 rcvdpkt=87 appcat="unscanned" sentdelta=7620 rcvddelta=5220
```

## Scenario 3

In this scenario, RSSO user *test2* in group *rsso-grp1* is authenticated on pc1, and user *test3* in group *rsso-grp2* is authenticated on pc2. Traffic flows from pc2 to pc1.

### Expected result:

In the logs, user *test3* is shown as the source user in the *rsso-grp1* group. User *test2* is shown as destination user (*dstuser*) in the *rsso-grp1* destination group (*dstgroup*). The destination group is logged because an RSSO user is logged in to pc2.

### To verify the results:

1. In the GUI, go to *Log & Report > Forward Traffic* and view the details of an entry with 172.16.200.185 (pc2) as the source.
2. In the *Source* section, *User* is *test3* and *Group* is the *rsso-grp2*. In the *Other* section, *Destination User* is *test2* and *Destination Group* is *rsso-grp1*.

Date/Time	Source	Device	Destination	Application N...	Result	Policy...	Log Details
2020/05/26 14:5...	test2 (10.1.100.188)	win7-2A-FortinetFSBO.COM	13.224.13.67 (mbada.difcon.e...		✓ 1.78 KB / 1.55 KB	port1 (1)	Log Details Source Interface: port9 User: test2 Group: rrsso-grp2
2020/05/26 14:5...	10.1.100.251	win2012-fsoo-3-FortinetFSBO.C...	10.8.36.16			dns (2)	Destination IP: 10.1.100.188 Port: 80 Destination MAC: 00:0c:29:44:be:b9 Country/Region: Reserved Destination Interface: port10
2020/05/26 14:5...	10.1.100.251	win2012-fsoo-3-FortinetFSBO.C...	172.16.200.142			dns (2)	
2020/05/26 14:5...	10.1.100.251	win2012-fsoo-3-FortinetFSBO.C...	10.8.36.124			dns (2)	
2020/05/26 14:5...	10.1.100.251	win2012-fsoo-3-FortinetFSBO.C...	10.8.36.131			dns (2)	
2020/05/26 14:5...	test2 (10.1.100.188)	win7-2A-FortinetFSBO.COM	172.16.200.16		✓ 197 B / 226 B	port1 (1)	
2020/05/26 14:5...	test2 (10.1.100.188)	win7-2A-FortinetFSBO.COM	172.16.200.16		✓ 197 B / 226 B	port1 (1)	
2020/05/26 14:5...	test2 (172.16.200...		10.1.100.188		✓ 328 B / 563 B	port2 (3)	Application Control Application Name: undefined Category: unscanned Risk: undefined Protocol: 6 Service: HTTP
2020/05/26 14:5...	test2 (172.16.200...		10.1.100.188		✓ 328 B / 563 B	port2 (3)	Stats Received Bytes: 563 B Received Packets: 5 Sent Bytes: 328 B Sent Packets: 6
2020/05/26 14:5...	test2 (172.16.200...		10.1.100.188		✓ 328 B / 563 B	port2 (3)	Action Action: Accept session close Policy ID: port2 (3) Policy: 5894c368-9eca-51ea-fb4c-ec5a6c1d5043 UID: ec5a6c1d5043 Policy Type: Firewall
2020/05/26 14:5...	test2 (172.16.200...		10.1.100.188		✓ 328 B / 563 B	port2 (3)	Security Level: [     ]
2020/05/26 14:5...	test2 (172.16.200...		10.1.100.188		✓ 328 B / 563 B	port2 (3)	Other Log ID: 0000000013 Type: traffic Sub Type: Forward Log event original timestamp: 1590528803131680000 Timezone: -0700 Source Interface Role: undefined Destination Interface Role: port2 Policy Name: undefined Authentication Server: vdom1 Destination User: test2 Destination Group: rrsso-grp1 Destination Authentication: vdom1
2020/05/26 14:5...	10.1.100.251	win2012-fsoo-3-FortinetFSBO.C...	172.16.200.131		✓ 15.25 MB / 203.33...	dns (2)	
2020/05/26 14:5...	test2 (172.16.200...		10.1.100.188		✓ 328 B / 563 B	port2 (3)	
2020/05/26 14:5...	win2012-fsoo-3-FortinetFSBO.C...		172.16.200.142		✓ 3.42 KB / 1.99 KB	dns (2)	
2020/05/26 14:5...	test2 (10.1.100.188)	win7-2A-FortinetFSBO.COM	60.147.60.15 (ads.yahoo.com)		✓ 2.44 KB / 1.71 KB	port1 (1)	

### 3. The log message shows both the source and the destination users and groups:

```
8: date=2020-05-25 time=14:23:07 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1590441786958007914 tz="-0700" srcip=172.16.200.185
srcport=64096 srcintf="port9" srcintfrole="undefined" dstip=10.1.100.188 dstport=80
dstintf="port10" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
sessionid=112445 proto=6 action="close" policyid=3 policytype="policy"
poluid="5894c368-9eca-51ea-fb4c-ec5a6c1d5043" policyname="pol2" user="test3"
group="rsso-grp2" authserver="vdom1" dstuser="test2" dstgroup="rsso-grp1"
dstauthserver="vdom1" service="HTTP" transip="snat" transip=10.1.100.1 transport=64096
duration=1 sentbyte=328 rcvbyte=563 sentpkt=6 rcvdpkt=5 appcat="unscanned"
dsthwvendor="VMware" dstosname="Windows" dstswversion="7"
masterdstmac="00:0c:29:44:be:b9" dstmac="00:0c:29:44:be:b9" dstserver=0
```

## Application logging in NGFW policy mode - 6.4.2

In NGFW policy mode, if an application, application category, or application group is selected on a security policy, and traffic logging is set to *UTM* or *All*, then application control logs will be generated. In addition, when a signature is set to the *ACCEPT* action under a security policy, all corresponding child signatures will be assessed and logged as well.

**To verify application logging:**

1. Go to *Policy & Objects > Security Policy* and configure a new policy for YouTube.
2. Set *Action* to **ACCEPT** and *Log Allowed Traffic* to **Security Events**.

3. Configure the remaining settings as required, then click **OK**.
4. On a client system, play some YouTube videos.
5. On FortiOS, go to *Log & Report > Application Control* and view the logs.  
There are logs not only for *YouTube*, but also for *YouTube\_Video.Play*, *YouTube\_Video.Access*, and so on, as verified from the *Application Name* column.

Add Filter							
Date/Time	Source	Destination	Application Name	Action	Application User	Details	
2020/06/26 16:55:50	10.1.100.199	209.52.146.47 (r4---sn-uxa0n-t8gs.googlevideo.com)	YouTube_Video.Play	pass		Video Play	
2020/06/26 16:55:50	10.1.100.199	209.52.146.47 (r4---sn-uxa0n-t8gs.googlevideo.com)	YouTube	pass			
2020/06/26 16:55:50	10.1.100.199	209.52.146.47 (r4---sn-uxa0n-t8gs.googlevideo.com)	YouTube_HD.Streaming	pass		HD Streaming	
2020/06/26 16:55:50	10.1.100.199	209.52.146.47 (r4---sn-uxa0n-t8gs.googlevideo.com)	YouTube	pass			
2020/06/26 16:55:49	10.1.100.199	216.58.193.78 (www.youtube.com)	YouTube_Channel.ID	pass	10.1.100.199	Channel ID: UCX	
2020/06/26 16:55:49	10.1.100.199	209.52.189.76 (r1---sn-uxa0n-t8gl.googlevideo.com)	YouTube_Video.Play	pass		Video Play	
2020/06/26 16:55:49	10.1.100.199	209.52.189.76 (r1---sn-uxa0n-t8gl.googlevideo.com)	YouTube_Video.Play	pass	10.1.100.199	Video Play: Can	
2020/06/26 16:55:49	10.1.100.199	209.52.189.76 (r1---sn-uxa0n-t8gl.googlevideo.com)	YouTube_HD.Streaming	pass		HD Streaming	
2020/06/26 16:55:49	10.1.100.199	209.52.189.76 (r1---sn-uxa0n-t8gl.googlevideo.com)	YouTube	pass			
2020/06/26 16:55:49	10.1.100.199	209.52.189.76 (r1---sn-uxa0n-t8gl.googlevideo.com)	YouTube	pass			
2020/06/26 16:55:49	10.1.100.199	216.58.193.78 (www.youtube.com)	YouTube_Video.Access	pass		Video Access	
2020/06/26 16:55:33	10.1.100.199	172.217.14.225 (yt3.ggpht.com)	YouTube	pass			
2020/06/26 16:55:31	10.1.100.199	216.58.193.86 (i.ytimg.com)	YouTube	pass			
2020/06/26 16:55:31	10.1.100.199	216.58.193.78 (www.youtube.com)	YouTube	pass			

## Send traffic logs to FortiAnalyzer Cloud - 6.4.4

FortiGates with a Premium subscription (AFAC) for Cloud-based Central Logging & Analytics, can send traffic logs to FortiAnalyzer Cloud in addition to UTM logs and event logs. After the Premium subscription is registered through FortiCare, FortiGuard will verify the purchase and authorize the AFAC contract. Once the contract is verified, FortiGuard will deliver the contract to FortiGate. Note that a FortiCloud Premium Account license is required to use this license.

FortiGates with a Standard FortiAnalyzer Cloud subscription (FAZC) can only send UTM and event logs. FortiGates with a Premium subscription will send the UTM and event logs even if the Standard subscription has expired.



FortiAnalyzer Cloud does not support DLP/IPS archives at this time.

## Example

In the following example, you will configure a FortiGate with a valid Premium subscription (AFAC) and expired Standard subscription (FAZC) to send traffic logs to FortiAnalyzer Cloud.

### 1. Configure the log delivery.

```
config log fortianalyzer-cloud setting
    set status enable
    set ips-archive disable
    set access-config enable
    set enc-algorithm high
    set ssl-min-proto-version default
    set conn-timeout 10
    set monitor-keepalive-period 5
    set monitor-failure-retry-period 5
    set certificate ''
    set source-ip ''
    set interface-select-method auto
    set upload-option realtime
    set priority default
    set max-log-rate 0
end
```

### 2. Verify the status of the FortiCloud Premium subscription (AFAC) and standard FortiAnalyzer Cloud subscription (FAZC).

The FAZC and AFAC fields display the subscription expiration date. The Support contract field displays the FortiCare account information. The User ID field displays the ID for FortiAnalyzer-Cloud instance.

```
# diagnose test update info
...
FAZC, Tue Sep 24 16:00:00 2030
AFAC, Mon Nov 29 16:00:00 2021
...
Support contract: pending_registration=255 got_contract_info=1
account_id=[****@fortinet.com] company=[Fortinet] industry=[Technology]
User ID: 979090
```

The FAZC and AFAC subscriptions are valid (date of verification is November 29, 2020).

### 3. Check the status of FortiAnalyzer Cloud.

```
# execute log fortianalyzer-cloud test-connectivity
FortiAnalyzer Host Name: FAZVM64-VIO-CLOUD
FortiAnalyzer Adom Name: root
FortiGate Device ID: FG101FTK19000000
Registration: registered
Connection: allow
Adom Disk Space (Used/Allocated): 50351453B/53687091200B
Analytics Usage (Used/Allocated): 41368925B/37580963840B
Analytics Usage (Data Policy Days Actual/Configured): 60/60 Days
Archive Usage (Used/Allocated): 8982528B/16106127360B
```

```

Archive Usage (Data Policy Days Actual/Configured): 235/365 Days
Log: Tx & Rx (log not received)
IPS Packet Log: Tx & Rx
Content Archive: Tx & Rx
Quarantine: Tx & Rx
Certificate of Fortianalyzer valid and serial number is:FAZVCLTM20000000

```

4. When the FortiCloud Premium (AFAC) and standard FortiAnalyzer Cloud (FAZC) subscriptions are valid, the FortiGate sends the traffic, event, and UTM logs to the remote FortiAnalyzer Cloud.

**Traffic:**

```

# execute log filter device fortianalyzer-cloud
# execute log filter category traffic
# execute log filter dump
category: traffic
device: fortianalyzer-cloud
start-line: 1
view-lines: 10
max-checklines: 0
HA member:
Oftp search string:
# execute log display
6512 logs found.
10 logs returned.
1: date=2020-11-29 time=13:57:33 id=6900668351836585985 itime="2020-11-29 13:57:34"
   euid=3 epid=1027 dsteuid=3 dstepid=101 logflag=1 logver=604041797 type="traffic"
   subtype="forward" level="notice" action="accept" policyid=1 sessionid=46536
   srcip=10.1.100.72 dstip=172.16.100.55 transip=172.16.200.7 srcport=40797 dstport=53
   transport=40797 trandisp="snat" duration=190 proto=17 sentbyte=268 rcvdbyte=0
   sentpkt=4 rcvdpkt=0 logid=0000000013 service="DNS" app="DNS" appcat="unscanned"
   srcintfrole="undefined" dstintfrole="undefined" srcserver=0 dstserver=0
   policytype="policy" eventtime=1606687054554969021 poluuid="c041939c-2930-51eb-1448-
   34c44a663331" srcmac="00:0c:29:eb:86:d6" mastersrcmac="00:0c:29:eb:86:d6"
   dstmac="e8:1c:ba:c2:86:63" masterdstmac="e8:1c:ba:c2:86:63" srchwvndor="VMware"
   osname="Linux" srccountry="Reserved" dstcountry="Reserved" srcintf="dmz"
   dstintf="wan1" policyname="to_WAN" tz="-0800" devid="FG101FTK19000000" vd="root"
   dtime="2020-11-29 13:57:33" itime_t=1606687054 devname="FortiGate-101F_F"

```

**Event:**

```

# execute log filter device fortianalyzer-cloud
# execute log filter category event
# execute log filter dump
category: event
device: fortianalyzer-cloud
start-line: 1
view-lines: 10
max-checklines: 0
HA member:
Oftp search string:
# execute log display
1067 logs found.
10 logs returned.
1: date=2020-11-29 time=14:12:16 id=6900672144292708352 itime="2020-11-29 14:12:17"
   euid=3 epid=3 dsteuid=3 dstepid=3 logver=604041797 logid=0100038404 type="event"
   subtype="system" level="error" msg="unable to resolve FortiGuard hostname"
   logdesc="FortiGuard hostname unresolvable" hostname="service.fortiguard.net"
   eventtime=1606687936888734117 tz="-0800" devid="FG101FTK19000000" vd="root"
   dtime="2020-11-29 14:12:16" itime_t=1606687937 devname="FortiGate-101F_F"

```

**UTM:**

```

# execute log filter device fortianalyzer-cloud

```

```
# execute log filter category utm-virus
# execute log filter dump
category: virus
device: fortianalyzer-cloud
start-line: 1
view-lines: 10
max-checklines: 0
HA member:
Oftp search string:
# execute log display
4 logs found.
4 logs returned.
1: date=2020-11-27 time=15:53:41 id=6899956121704857638 itime="2020-11-27 15:53:45"
  euid=1027 epid=101 dsteuid=3 dstepid=101 logver=604041797 type="utm"
  subtype="virus" level="warning" action="passthrough" sessionid=1957747803
  policyid=1 srcip=168.10.199.186 dstip=172.252.3.20 srcport=22765 dstport=80 proto=6
  vrf=32 logid=0212008448 service="NNTP" user="user3" group="group1"
  eventtime=1606521221884991620 crscore=5 craction=2 crlevel="low"
  srcintfrole="undefined" dstintfrole="undefined" direction="incoming"
  filefilter="file-pattern" filetype="ignored" filename="file_test" checksum="12345"
  eventtype="filename" srcintf="ssl.root" dstintf="x1" msg="File is blocked." tz="-
0800" devid="FG101FTK19000000" vd="root" dtime="2020-11-27 15:53:41" itime_
t=1606521225 devname="FortiGate-101F_F"
```

5. When the FortiGate has a valid Premium FortiCloud subscription (AFAC) and an expired Standard FortiCloud subscription (FAZC), the FortiGate still sends the logs to the remote FortiAnalyzer Cloud.

## Log updates to dynamic objects - 6.4.5

EMS logs are recorded for dynamic address related events, including adding, updating, and removing EMS tags.

The dynamic address list includes EMS tags, such as the MAC tag:

```
# diagnose firewall dynamic list

MAC_FCTEMSTA20002318_ems135_winOS_tag(total-addr: 2): ID(62) TAG()
  MAC(02:00:4C:4F:4F:50)
  MAC(64:00:6A:8E:95:62)
```



## To view the logs in the GUI:

### 1. Go to *Log & Report > Events* and select *SDN Connector Events*:

#	Date/Time	Log Description	Address	Device ID	Level	Message	Log ID	Vir
2	15 minutes ago	Dynamic address added	FCTEM50000101519_Medium	FG2KSE	Information	Created new tag FCTEM50000101519_Medium.	53200	
3	15 minutes ago	Dynamic address added	MAC_FCTEM50000101519_Low	FG2KSE	Information	Created new tag MAC_FCTEM50000101519_Low.	53200	
4	15 minutes ago	Dynamic address added	FCTEM50000101519_Low	FG2KSE	Information	Created new tag FCTEM50000101519_Low.	53200	
5	15 minutes ago	Dynamic address added	MAC_FCTEM50000101519_High	FG2KSE	Information	Created new tag MAC_FCTEM50000101519_High.	53200	
6	15 minutes ago	Dynamic address added	FCTEM50000101519_High	FG2KSE	Information	Created new tag FCTEM50000101519_High.	53200	
7	15 minutes ago	Dynamic address added	MAC_FCTEM50000101519_Critical	FG2KSE	Information	Created new tag MAC_FCTEM50000101519_Critical.	53200	
8	15 minutes ago	Dynamic address added	FCTEM50000101519_Critical	FG2KSE	Information	Created new tag FCTEM50000101519_Critical.	53200	
9	15 minutes ago	Dynamic address added	MAC_FCTEM50000101519_cloud_ems_winos_tag	FG2KSE	Information	Created new tag MAC_FCTEM50000101519_cloud_ems_winos_tag.	53200	
10	15 minutes ago	Dynamic address added	FCTEM50000101519_cloud_ems_winos_tag	FG2KSE	Information	Created new tag FCTEM50000101519_cloud_ems_winos_tag.	53200	
11	15 minutes ago	Dynamic address added	MAC_FCTEM50000101519_cloud_ems_macos_tag	FG2KSE	Information	Created new tag MAC_FCTEM50000101519_cloud_ems_macos_tag.	53200	
12	15 minutes ago	Dynamic address added	FCTEM50000101519_cloud_ems_macos_tag	FG2KSE	Information	Created new tag FCTEM50000101519_cloud_ems_macos_tag.	53200	
13	2 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
14	2 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
15	3 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
16	3 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
17	3 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
18	3 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
19	4 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
20	4 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
21	4 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
22	4 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
23	5 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
24	5 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
25	5 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
26	2021/02/11 19:52:33	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
27	5 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
28	5 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	
29	6 hours ago	Dynamic address updated	FCTEM5_ALL_FORTICLOUD_SERVERS	FG2KSE	Information	Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS.	53203	

## To view the logs in the CLI:

```
# execute log filter device 2
# execute log filter category 1
# execute log filter field subtype connector
# execute log display
112 logs found.
10 logs returned.
```

```
1: date=2021-02-11 time=15:12:29 id=6928147977798156362 itime="2021-02-11 15:12:33" euid=3
epid=3 dsteuid=3 dstepid=3 logver=604051825 logid=0112053203 type=event subtype=connector
level=information msg="Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS." logdesc="Dynamic address
updated" addr=FCTEM5_ALL_FORTICLOUD_SERVERS eventtime=1613085150627684117 fctemssn=(null)
tz=-0800 devid=FWF61ETK20001713 vd=root csf=EC_61E_Faric dtime="2021-02-11 15:12:29" itime_
t=1613085153 devname=EC_61E
```

```
2: date=2021-02-11 time=15:12:30 id=6928147964913254410 itime="2021-02-11 15:12:30" euid=3
epid=3 dsteuid=3 dstepid=3 logver=604051825 logid=0112053203 type=event subtype=connector
level=information msg="Updated tag FCTEM5_ALL_FORTICLOUD_SERVERS." logdesc="Dynamic address
updated" addr=FCTEM5_ALL_FORTICLOUD_SERVERS eventtime=1613085150686659727 fctemssn=(null)
tz=-0800 devid=FWF61ETK18002255 vd=root csf=EC_61E_Faric dtime="2021-02-11 15:12:30" itime_
t=1613085150 devname=EC_61E
...
```

## Log examples

### Dynamic address added

```
10: date=2021-02-10 time=17:34:28 eventtime=1613007268451987782 tz="-0800"
logid="0112053200" type="event" subtype="connector" level="information" vd="root"
logdesc="Dynamic address added" fctemssn="FCTEMSTA20002318" addr="FCTEMSTA20002318_all_
registered_clients" msg="Created new tag FCTEMSTA20002318_all_registered_clients."
```

### Dynamic address expired removed

```
11: date=2021-02-10 time=17:33:29 eventtime=1613007209497390822 tz="-0800"  
logid="0112053201" type="event" subtype="connector" level="information" vd="root"  
logdesc="Dynamic address removed" fctemssn="FCTEMSTA20002318" addr="all_registered_clients"  
msg="Removed expired tag all_registered_clients."
```

### Dynamic address updated

```
14: date=2021-02-10 time=17:27:19 eventtime=1613006839576044092 tz="-0800"  
logid="0112053203" type="event" subtype="connector" level="information" vd="root"  
logdesc="Dynamic address updated" fctemssn="FCTEMSTA20002318" addr="FCTEMSTA20002318_all_  
registered_clients" msg="Updated tag FCTEMSTA20002318_all_registered_clients."
```

### Dynamic address removed

```
30: date=2021-02-10 time=11:38:40 eventtime=1612985920771374086 tz="-0800"  
logid="0112053201" type="event" subtype="connector" level="information" vd="vdom1"  
logdesc="Dynamic address removed" fctemssn="FCTEMSTA20002318" addr="MAC_FCTEMSTA20002318_  
Critical" msg="Removed tag MAC_FCTEMSTA20002318_Critical."
```

# Cloud

This section includes information about cloud related new features:

- [Public and private cloud on page 501](#)

## Public and private cloud

This section includes information about public and private cloud related new features:

- [Simplify Azure Fabric connector configuration for a FortiGate-VM deployed on Azure on page 501](#)
- [Support filtering on AWS autoscaling group for dynamic address objects on page 504](#)
- [Support dynamic address objects in real servers under virtual server load balance on page 505](#)
- [Support up to 24 interfaces on FortiGate VM on page 506](#)
- [Enhanced autoscale clusters for FortiGate VM on page 508](#)
- [Support FortiGate-VM in IBM Cloud platform 6.4.2 on page 509](#)
- [Obtaining a FortiCare-generated license for Azure on-demand instances 6.4.2 on page 514](#)
- [Configure FQDN-based VIPs from the GUI 6.4.2 on page 515](#)
- [Enhance the display of VM autoscale member information 6.4.2 on page 516](#)
- [Support for new VM bandwidth-limited SKUs 6.4.2 on page 517](#)
- [FOS support of VM-ELA \(FortiFlex\) 6.4.2 on page 521](#)
- [Liveness detection on NSX-T 6.4.3 on page 523](#)
- [Add FIPS cipher mode for AWS and Azure FortiGate VMs 6.4.3 on page 523](#)
- [IMDSv2 for FortiGate-VM on AWS 6.4.3 on page 525](#)
- [Add VDOM support for NSX-T 6.4.3 on page 525](#)
- [Support OCI compute shapes that use Mellanox network cards 6.4.3 on page 527](#)
- [Support AWS transit gateway connect attachment and connect peer 6.4.3 on page 530](#)
- [Support OCI IMDSv2 6.4.4 on page 534](#)
- [GENEVE support for AWS gateway load balancer 6.4.4 on page 537](#)
- [Nutanix service chaining 6.4.5 on page 538](#)
- [Support multiple GCP projects in a single SDN connector 6.4.7 on page 545](#)
- [Ciphers added to fips-ciphers mode on FortiGate-VM 6.4.7 on page 549](#)

## Simplify Azure Fabric connector configuration for a FortiGate-VM deployed on Azure

For a FortiGate-VM deployed on Azure, the new *Use managed identity* setting allows FortiOS to connect to Azure based on the FortiGate-VM's user-assigned managed identity. Using user-assigned managed identities enables a FortiGate-VM deployed on Azure to authenticate to cloud services without storing credentials in FortiOS.

When you enable *Use managed identity* for an Azure Fabric connector, you do not need to configure the *Tenant ID*, *Client ID*, and *Client secret* fields on the Fabric connector creation page. FortiOS hides these fields when you enable *Use managed identity* for an Azure Fabric connector.

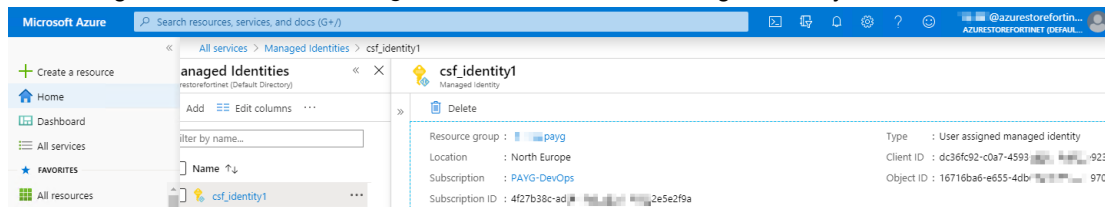
This feature only applies for a FortiGate-VM deployed on Azure. For a FortiGate that is not deployed on Azure, you must still configure the *Tenant ID*, *Client ID*, and *Client secret* fields for an Azure Fabric connector. This feature also does not apply for a FortiGate-VM deployed on Azure Stack.

This configuration consists of the following steps:

1. [Configure a user-managed identity in Azure.](#)
2. Configure an Azure Fabric connector in FortiOS:
  - a. [GUI instructions](#)
  - b. [CLI instructions](#)

### To configure a user-managed identity in Azure:

1. In Azure, go to *All services > Managed Identities*. Create a managed identity.



2. Go to the FortiGate-VM instance, then go to *Identity*. Set the managed identity created in step a as the user-assigned identity.
3. Search for subscriptions to assign the level of scope. Select the subscription, then go to *Access control (IAM)*. Click *Add role assignment*. From the *Role* dropdown list, select *Contributor*.

### To configure an Azure Fabric connector in the FortiOS GUI:

1. Configure the Fabric connector in FortiOS:
  - a. On the FortiGate-VM deployed on Azure, go to *Security Fabric > External Connectors*.
  - b. Click *Create New*.
  - c. Under *Public SDN*, select *Microsoft Azure*.
  - d. Enable *Use managed identity*.
  - e. Configure other settings as desired.
  - f. Click *OK*.
2. Create a dynamic firewall address associated to the Fabric connector:
  - a. Go to *Policy & Objects > Addresses*.
  - b. From the *Type* dropdown list, select *Dynamic*.
  - c. From the *Sub Type* dropdown list, select *Fabric Connector Address*.
  - d. From the *SDN Connector* dropdown list, select the Fabric connector that you created in step 1.
  - e. Configure other settings as desired.
  - f. Click *OK*.
3. To confirm that the Fabric connector resolves the dynamic firewall IP addresses with the supported filter, go to

**Policy & Objects > Addresses.** Hover over the address that you created in step 2.

Name	Type	Details	Interface	Visibility	Ref.
aws-address-group1	Dynamic (AWS)			Visible	1
azure-iam-1	Dynamic (AZURE)			Visible	0
gcp-address	Dynamic (GCP)			Visible	0
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0

## To configure an Azure Fabric connector in the FortiOS CLI:

### 1. Configure the Fabric connector in FortiOS:

```
config system sdn-connector
  edit "azure"
    set status enable
    set type azure
    set azure-region global
    set use-metadata-iam enable
  next
end
```

### 2. Create a dynamic firewall address associated to the Fabric connector:

```
config firewall address
  edit "azure-iam-1"
    set type dynamic
    set sdn "azure"
    set color 2
    set filter "ResourceGroup=azuretest"
  next
end
```

### 3. Confirm that the Fabric connector resolves the dynamic firewall IP addresses with the supported filter:

```
config firewall address
  edit "azure-iam-1"
    set type dynamic
    set sdn "azure2"
    set color 2
    set filter "ResourceGroup=azuretest"
  config list
    edit "10.0.0.4"
    next
    edit "10.0.0.5"
    next
    edit "10.0.1.10"
    next
    edit "10.0.1.4"
    next
    edit "10.0.1.5"
    next
    edit "10.0.2.10"
    next
    edit "10.0.2.4"
    next
    edit "10.0.2.5"
```

```

next
edit "10.0.3.10"
next
edit "10.0.3.4"
next
edit "10.0.3.5"
next
edit "10.5.0.4"
next
edit "10.5.0.5"
next
edit "10.8.0.5"
next
edit "10.8.1.6"
next
end
next
end

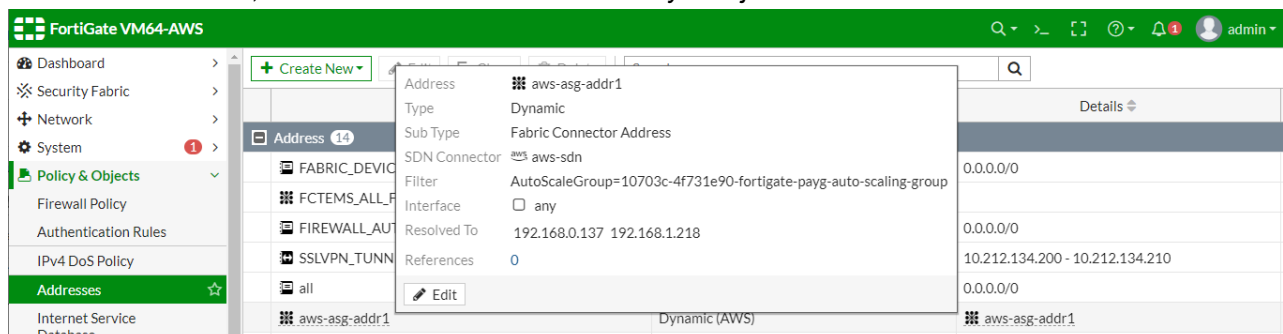
```

## Support filtering on AWS autoscaling group for dynamic address objects

A FortiGate-VM deployed on AWS can create a dynamic address based on an AWS Fabric connector and use an autoscaling group (ASG) filter to obtain ASG members' primary IP addresses or NICs. You can use this feature for load balancing to optimize network efficiency.

### To create an address with an ASG filter using the GUI:

1. In FortiOS, go to *Policy & Objects > Addresses*.
2. Click *Create New*, then select *Address*.
3. Enter the address name. From the *Type* dropdown list, select *Dynamic*.
4. From the *Sub Type* dropdown list, select *Fabric Connector Address*.
5. From the *SDN Connector* dropdown list, select the AWS Fabric connector.
6. In the *Filter* fields, enter the desired filter. In this example, you would enter `AutoScaleGroup=<ASG ID>` in the *Filter* field.
7. From the *Interface* dropdown list, select an interface where the Fabric connector covers where relevant.
8. Click *OK*. Once saved, FortiOS lists the address under *Policy & Objects > Addresses*.



### To create an address with an ASG filter using the CLI:

```

config firewall address
edit "aws-asg-addr1"

```

```

set uuid 82e26cea-756e-51ea-d322-4259d3db301b
set type dynamic
set sdn "aws-sdn"
set filter "AutoScaleGroup=10703c-4f731e90-fortigate-payg-auto-scaling-group"
config list
  edit "192.168.0.137"
  next
  edit "192.168.1.218"
  next
end
next
end

```

## Support dynamic address objects in real servers under virtual server load balance

FortiOS supports using dynamic firewall addresses in real servers under a virtual server load balancing configuration. Combined with support for the autoscaling group filter (see [Support filtering on AWS autoscaling group for dynamic address objects on page 504](#)), this enables you to use the FortiGate as a load balancer in AWS for an autoscaling deployment. You do not need to manually change each server's IP address whenever a scale in/out action occurs, as FortiOS dynamically updates the IP addresses following each scale in/out action.

Consider a scenario where the FortiGate-VM is deployed on AWS and load balancing for three servers. The Fabric connector configured in FortiOS dynamically loads the server IP addresses. If a scale in action occurs, the load balancer dynamically updates to load balance to the two remaining servers.

The following instructions assume the following:

1. An AWS Fabric connector is configured and up.
2. An AWS dynamic firewall address with a filter is configured.

### To configure a dynamic address object in a real server under virtual server load balance:

CLI commands introduced in FortiOS 6.4.0 are shown bolded below.

```

config firewall vip
  edit "0"
    set id 0
    set uuid 0949dfbe-7512-51ea-4671-d3a706b09657
    set comment ''
    set type server-load-balance
    set extip 0.0.0.0
    set extintf "port1"
    set arp-reply enable
    set server-type http
    set nat-source-vip disable
    set gratuitous-arp-interval 0
    set http-ip-header disable
    set color 0
    set ldb-method static
    set http-redirect disable
    set persistence none
    set extport 80
    config realservers
      edit 1
        set type address
        set address "aws addresses"

```

```

        set port 8080
        set status active
        set holddown-interval 300
        set healthcheck vip
        set max-connections 0
        unset client-ip
    next
end
set http-multiplex disable
set max-embryonic-connections 1000
next
end

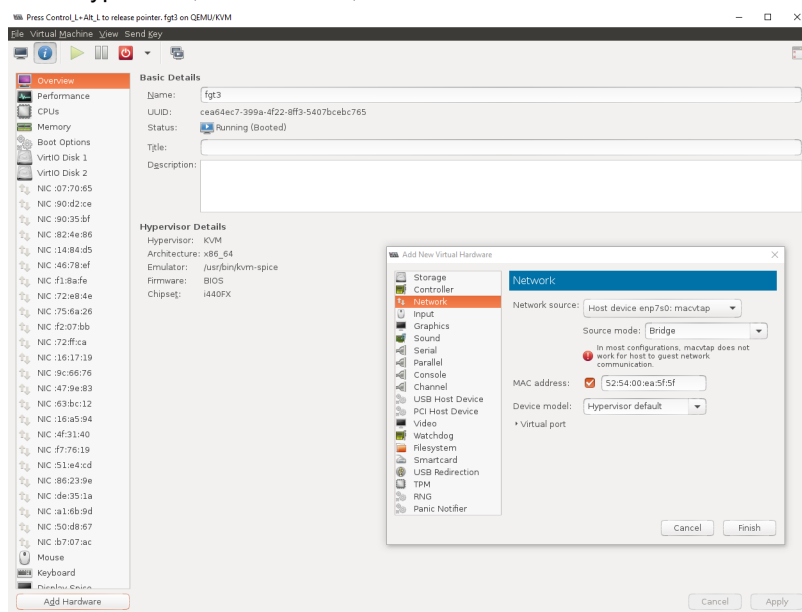
```

## Support up to 24 interfaces on FortiGate VM

FortiGate VM now supports 24 interfaces or ports.

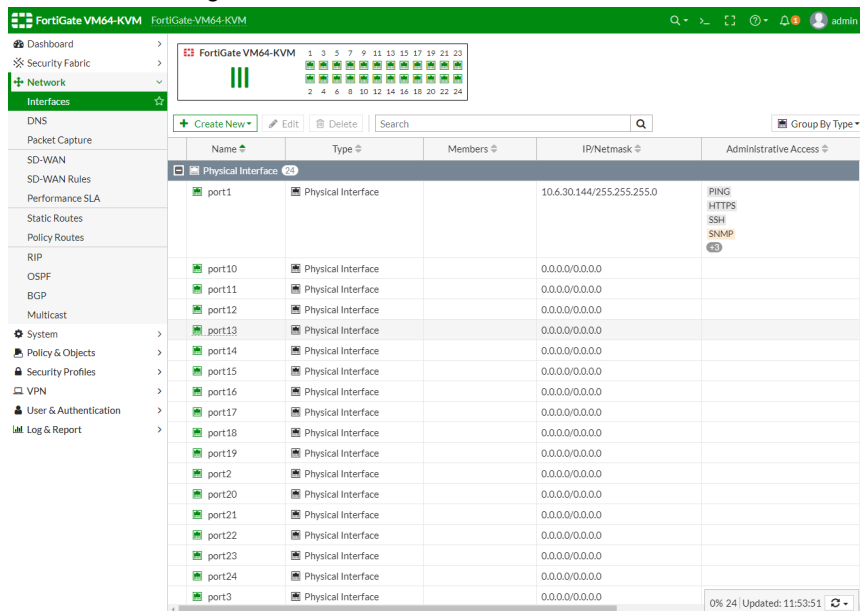
### To use all 24 interfaces:

1. In the hypervisor, such as KVM, create 24 interfaces.





2. On the FortiGate, go to *Network > Interfaces* to see all of the available interfaces.



3. In the CLI, enter the following command to see the interfaces:

```
# show system interface
config system interface
  edit "port1"
    set vdom "root"
    set ip 10.6.30.144 255.255.255.0
    set allowaccess ping https ssh snmp http telnet fgfm
    set type physical
    set snmp-index 1
  next
  edit "port2"
    set vdom "root"
    set type physical
    set snmp-index 3
  next
  ...
  edit "port23"
    set vdom "root"
    set type physical
    set snmp-index 24
  next
  edit "port24"
    set vdom "root"
    set type physical
    set snmp-index 25
  next
  edit "ssl.root"
    set vdom "root"
    set type tunnel
    set alias "SSL VPN interface"
    set snmp-index 2
```

```

    next
end

```

## Enhanced autoscale clusters for FortiGate VM

This improvement supports the visibility of autoscale VM clusters on FortiManager, and its ability to read cluster information from new secondary members.

When a FortiGate VM secondary is added to a cluster, the new secondary member can query the cluster about its autoscale environment. FortiManager can then run this query on the new secondary member to update its autoscale record.

### To view cluster information from a secondary member:

```
# diagnose sys ha checksum autoscale-cluster
```

### Cluster information sample

#### Sample cloud topology:

```
FGT_BYOL; primary; 10.0.0.6; FGVM04TM000000066
FGT_BYOL; secondary; 10.0.0.7; FGVM00000000056
FGT_PAYG; secondary; 10.0.0.4; FGTAZ000000000CD
FGT_PAYG; secondary; 10.0.0.5; FGTAZ0000000003D
```

From the secondary, you can see cluster checksums and the primary device.

```
# diagnose sys ha checksum autoscale-cluster
===== FGTAZ000000000CD =====
is_autoscale_master()=0
debugzone
global: 56 49 b3 02 f2 b7 5b 82 ec 2d c2 1a ff 80 8c 79
root: bf 18 cf 83 1e 04 c3 04 4c e4 66 bc 38 fe 3a dc
all: 77 06 d0 89 6e 06 c0 86 17 98 53 72 33 85 ae ff
checksum
global: 56 49 b3 02 f2 b7 5b 82 ec 2d c2 1a ff 80 8c 79
root: bf 18 cf 83 1e 04 c3 04 4c e4 66 bc 38 fe 3a dc
all: 77 06 d0 89 6e 06 c0 86 17 98 53 72 33 85 ae ff
===== FGVM04TM000000066 =====
is_autoscale_master()=1
debugzone
global: 56 49 b3 02 f2 b7 5b 82 ec 2d c2 1a ff 80 8c 79
root: bf 18 cf 83 1e 04 c3 04 4c e4 66 bc 38 fe 3a dc
all: 77 06 d0 89 6e 06 c0 86 17 98 53 72 33 85 ae ff
checksum
global: 56 49 b3 02 f2 b7 5b 82 ec 2d c2 1a ff 80 8c 79
root: bf 18 cf 83 1e 04 c3 04 4c e4 66 bc 38 fe 3a dc
all: 77 06 d0 89 6e 06 c0 86 17 98 53 72 33 85 ae ff
===== FGVM00000000056 =====
is_autoscale_master()=0
debugzone
global: 56 49 b3 02 f2 b7 5b 82 ec 2d c2 1a ff 80 8c 79
root: bf 18 cf 83 1e 04 c3 04 4c e4 66 bc 38 fe 3a dc
all: 77 06 d0 89 6e 06 c0 86 17 98 53 72 33 85 ae ff
checksum
```

```

global: 56 49 b3 02 f2 b7 5b 82 ec 2d c2 1a ff 80 8c 79
root: bf 18 cf 83 1e 04 c3 04 4c e4 66 bc 38 fe 3a dc
all: 77 06 d0 89 6e 06 c0 86 17 98 53 72 33 85 ae ff
===== FGTAZ0000000003D =====
is_autoscale_master()=0
debugzone
global: 56 49 b3 02 f2 b7 5b 82 ec 2d c2 1a ff 80 8c 79
root: bf 18 cf 83 1e 04 c3 04 4c e4 66 bc 38 fe 3a dc
all: 77 06 d0 89 6e 06 c0 86 17 98 53 72 33 85 ae ff
checksum
global: 56 49 b3 02 f2 b7 5b 82 ec 2d c2 1a ff 80 8c 79
root: bf 18 cf 83 1e 04 c3 04 4c e4 66 bc 38 fe 3a dc
all: 77 06 d0 89 6e 06 c0 86 17 98 53 72 33 85 ae ff

```

### To get ha sync information from the secondary:

```
# get test hasync 50
```

#### HA sync information:

```

autoscale_count=69. current_jiffies=41235125
  10.0.0.6, timeo=31430, serial_no=FGVM04TM19001766
  10.0.0.7, timeo=31430, serial_no=FGVM04TM19008156
  10.0.0.5, timeo=31430, serial_no=FGTAZR7UZRKKNR3D
connections = 0

```

## Support FortiGate-VM in IBM Cloud platform - 6.4.2


FortiOS 6.4.2 adds support for deploying FortiGate-VM BYOL for the IBM Cloud platform. IBM Cloud platform users can purchase and deploy FortiGate-VMs. The following describes the steps that you take to create and access a FortiGate-VM BYOL instance in the IBM Cloud.

### To deploy FortiGate-VM on IBM Cloud using the GUI:

1. Obtain the .qcow2 image file:
  - a. Log in to the [Fortinet Support site](#).
  - b. Go to *Download > VM Images*.
  - c. From the *Select Platform* dropdown list, select *IBM VPC Cloud*.
  - d. Download the FortiGate-VM deployment file (FGT\_VM64\_IBM-v6-buildXXXX-FORTINET.out.kvm.zip).
  - e. Extract the zip file to get a .qcow2 file.
2. Log in to the IBM Cloud portal.
3. Prepare an object storage bucket on IBM VPC.
4. Upload the .qcow2 image file.
5. Import the custom image:
  - a. Go to *VPC Infrastructure (Gen 2) > Compute > Custom images*.
  - b. Click *Import custom image*.
  - c. Import the custom image. You must enter a name and select a region. Select the .qcow2 image file uploaded

earlier, and select Ubuntu 16.04 for the operating system.

VPC Infrastructure / All custom images for VPC



**Gen 2 compute**

This custom image will be created for use with generation 2 compute resources. It cannot be used with generation 1 instances.

[Switch to Gen 1 compute](#)

## Import custom image

**Name**

fortios1705

**Resource group**

The resource group can't be changed after the custom image is created

[Learn about resource groups](#)

Default

[View all resource groups](#)

**Tags**

Examples: env:dev, version-1

**Region**

Dallas

Frankfurt

London

Washington DC

Select your Cloud Object Storage bucket and select your image file below. [How to upload to Cloud Object Storage.](#)

Images must be a qcow2 file type, 100GB or less and cloud-init enabled.

Cloud Object Storage instances	Location	Bucket
thomasobjectstore	us-east	thomasbucket

Prefix filter

Name	Size	Last Modified
fortios.qcow2	58.63 MB	July 9, 2020 12:23:19 PM

Items per page: 10 1 item Page 1

**Operating system**

CentOS  
7.x - Minimal Install

Debian GNU/Lin...  
debian-8-amd64

Red Hat Enterpr...  
7.x - Minimal Install

Ubuntu Linux  
ubuntu-16-04-amd64

Windows Server  
windows-2012-amd

**Summary** United States

**1 Image** \$0.01

0.06 GB

Apply a code

Apply

**Total monthly cost\*** \$0.01  
*estimated*

Import custom image

Get sample API call

Add to estimate

**Need help?**

[Contact IBM Cloud Sales](#)

[View docs](#)

**Terms**

[Virtual Server](#)

[Virtual Private Cloud](#)

[Block Storage](#)

FEEDBACK

6. Create a new instance based on the custom image. Enter a name, select the VPC, location, custom image imported earlier, profile, SSH key, and user data. User data can be from the IBM bucket, config-url/license-url, or directly inputted in the form of a config, license, or MIME file. See the following example:

```
{
  "bucket" : "lzou-bucket1",
  "region" : "eu-gb",
  "license" : "FGVM16TM19000211.lic",
  "config" : "config.txt",
  "apikey": "{{omitted}}"
}
```

The following example includes the license-url and config-url:

```
{
  "license-url" : "http://ec2-54-151-72-112.us-west-1.compute.amazonaws.com/FGVM16TM19000211.lic",
  "config-url" : "http://ec2-54-151-72-112.us-west-1.compute.amazonaws.com/config.txt" }
}
```

IBM Cloud

Search Catalog Docs Support Manage

## New virtual server for VPC

Name

fosinstance

Virtual private cloud

thomas-vpc-general

Resource group

The resource group can't be changed after the virtual server instance is created

[Learn about resource groups](#)

Default

Tags

Examples: env:dev, version-1

Location

Washington DC

Washington DC 1

Image

CentOS

7.x - Minimal Install

Debian GNU/Linux

9.x Stretch/Stable - Minimal Install

Red Hat Enterprise Linux

7.x - Minimal Install

Ubuntu Linux

18.04 LTS Bionic Beaver

Windows Server

2016 Standard Edition

fortios1705

Change image

Catalog image

Select catalog image

Popular profiles

All profiles

Balanced

Best for common cloud workloads

8 vCPUs

32 GB RAM

16 Gbps

Compute

Best for workloads with intensive CPU demands

2 vCPUs

4 GB RAM

4 Gbps

Memory

Best for memory intensive workloads

2 vCPUs

16 GB RAM

4 Gbps

SSH keys

thomas-myfirstkeypair

New key

User data (optional)

Paste user data

Import user data

Boot volume

Volume Size Max Throughput Encryption Auto

Summary

United States

1 Virtual server instance

2 vCPUs  
4 GB RAM  
4 Gbps  
Custom image

\$0.09/hr

Boot volume

100 GB

\$0.02/hr

Network interface

provided

Apply a code

Apply

Subtotal \$78.04

Sustained usage discount -\$6.58

Total monthly cost\* \$71.46 estimated

Create virtual server instance

Get sample API call

Add to estimate

Need help?

Contact IBM Cloud Sales

View docs

Terms

Virtual Server

Virtual Private Cloud

Block Storage

FEEDBACK

FortiOS 6.4.0 New Features Guide  
Fortinet Inc.

512

7. Attach a floating IP address to the instance NIC.
8. In a browser, go to the IP address to connect to the FortiOS GUI and confirm that the instance is running.

### To deploy FortiGate-VM on IBM Cloud using the CLI:

```
ibmcloud # diagnose debug cloudinit show
>> Checking metadata source ibm
>> Found nocloud drive /dev/vdb
>> Successfully mounted nocloud drive
>> Setting password to instance id
>> Provisioning ssh key
>> Cloudinit curl header:
>> Cloudinit trying to get license from:
    https://thomasgabucket2.s3.amazonaws.com/FGVM08TM20004028.lic
>> Cloudinit download license successfully
>> Cloudinit trying to get config script from:
    https://thomasgabucket2.s3.amazonaws.com/config2.txt
>> Cloudinit download config script successfully
>> Found metadata source: ibm
>> Trying to install vmlicense ...
>> Run config script
>> Finish running script
>> FGVM08TM20004028 $ config system global
>> FGVM08TM20004028 (global) $ set hostname ibmcloud
>> FGVM08TM20004028 (global) $ end

get system status
Version: FortiGate-VM64-IBM v6.4.0,buidl1705,200708 (interim)
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
Serial-Number: FGVM08TM20004028
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
License Status: Valid
License Expiration Date: 2021-05-15
VM Resources: 2 CPU/8 allowed, 3689 MB RAM
Log hard disk: Not available
Hostname: ibmcloud
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1705
Release Version Information: interim
FortiOS x86-64: Yes
System time: Thu Jul 9 15:14:00 2020
```

## Obtaining a FortiCare-generated license for Azure on-demand instances - 6.4.2

New Azure on-demand and upgraded instances can retrieve a FortiGate serial number and license from FortiCare servers. Using the serial number, users can register the device to their account and start using FortiToken and FortiGate Cloud services.

The FortiGate-VM must be able to reach FortiCare to receive a valid on-demand license. Ensure connectivity to FortiCare (<https://directregistration.fortinet.com/>) by checking all related setup on the virtual network, subnet, network security group, route table, public IP addresses, and so on.

### To verify cloudinit automatically obtained a license for a newly-deployed instance:

```
# diagnose debug cloudinit show
>> Load VM metadata document
>> Requesting FortiCare license: FGTAZRXXXXXXXXXX
>> VM license install succeeded. Rebooting firewall.
```

```
# diagnose debug vm-print-license
SerialNumber: FGTAZRXXXXXXXXXX
CreateDate: Wed Jul 29 16:48:34 2020
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: PG (20)
CPU: 2147483647
MEM: 2147483647
```

```
# execute vm-license
PAYG license exists.
```

If in a closed network, the command execution resembles the following, as the `execute vm-license` command attempts to get a license from FortiCare.

```
# diagnose debug cloudinit show

# diagnose debug vm-print-license
SerialNumber: FGTAZRXXXXXXXXXX
CreateDate: 1597362903
Model: PG (20)
CPU: 2147483647
MEM: 2147483647

# execute vm-license
This operation will reboot the system !
Do you want to continue? (y/n)
```

```
Load VM metadata document
Requesting FortiCare license: FGTAZRXXXXXXXXXX
```

If the FortiGate-VM connects to FortiCare successfully, the following message displays.

```
VM license install succeeded. Rebooting firewall.
```



### To obtain a license for an upgraded instance or instance from a closed network:

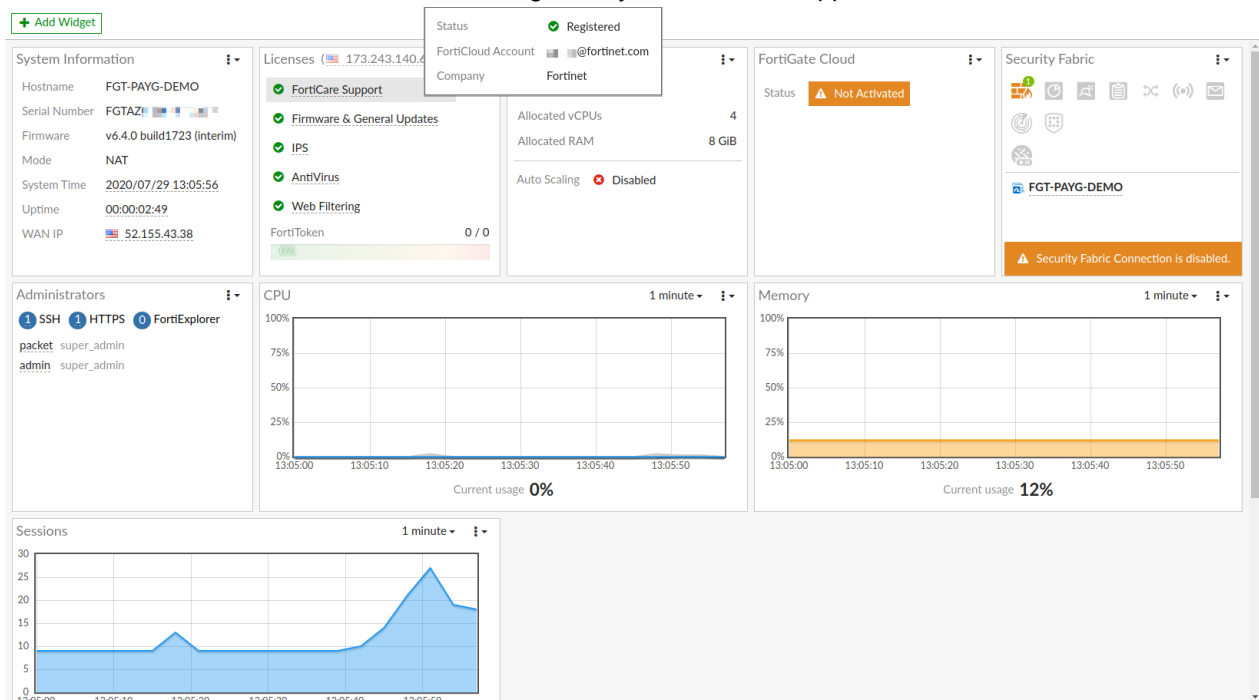
If you created the FortiGate-VM in a closed environment or it cannot reach FortiCare, the FortiGate-VM self-generates a local license as in previous FortiOS versions. You can obtain a FortiCare license, ensure that the FortiGate-VM can connect to FortiCare, then run the `execute vm-license` command to obtain the license from FortiCare.

```
# execute vm-license
This operation will reboot the system !
Do you want to continue? (y/n)y

Load VM metadata document
Requesting FortiCare license: FGTAZRXXXXZXXXXXX
VM license install succeeded. Rebooting firewall.
```

### To register the serial number:

1. Register the license using the serial number in FortiCare (see [Creating a support account](#)).
2. Obtain the VM ID:
  - In FortiOS, run `diagnose test application azd 6` and search for the VM Instance ID.
  - In Azure, run `az vm show -g Resource-Group-Name -n PAYG-VM-Name --query vmId -o tsv`.  
It may take up to an hour for the registration status to synchronize and update in the FortiOS GUI.
3. Go **Dashboard > Status** and in the **Licenses** widget verify the **FortiCare Support** status.



4. Once the registration is complete, you can log in to a [FortiGate Cloud](#) account and download the two free tokens that come standard with FortiGates (see [FortiTokens](#)).

## Configure FQDN-based VIPs from the GUI - 6.4.2

In public cloud environments, sometimes it is necessary to map a VIP to an FQDN address. This setting can now be configured from the GUI.

### To configure an FQDN-based VIP:

1. Go to *Policy & Objects > Virtual IPs* and click *Create New > Virtual IP*.
2. Enter a name for the VIP.
3. Select an interface.
4. For *Type*, select *FQDN*.
5. Enter the external IP address.
6. For *Mapped address*, select an FQDN address.

7. Click **OK**.

In the virtual IP list, hover over the address to view more information.

<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Delete</a> <input type="text" value="Search"/>						
Name	Details	Interfaces	Services	Ref.	External IP Address/Range	Mapped IP Address/Range/FQDN
IPv4 Virtual IP						
FQDN-vip-1	10.2.2.199 → destination	any		0	10.2.2.199	destination

Address destination  
 Type FQDN  
 FQDN pc4.qa.fortinet.com  
 Interface any  
 Resolved To 172.16.200.44  
 References 1  
[Edit](#)

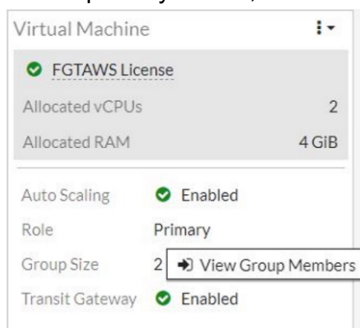
## Enhance the display of VM autoscale member information - 6.4.2

Information about autoscale members such as their serial number, IP address, instance ID, and transit gateway (AWS only) is displayed in the GUI and CLI.

### GUI

In the *Dashboard > Status* page, the *Virtual Machine* widget displays autoscale member information.

- On the primary device, click the *View Group Members* drilldown to view group member information:

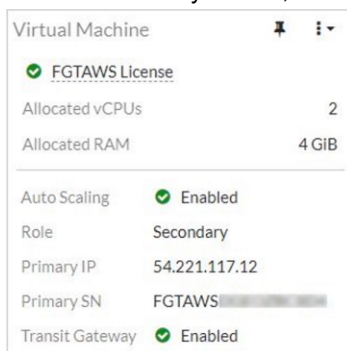


In the members table, hover over the *Transit Gateway* to display a tooltip:

Active Autoscale Members			
Serial Number	IP Address	Ins	Transit Gateway
FGTAWs	Unknown		tgw-vpn-2

IPsec Tunnel + tgw-vpn-2  
 Remote Gateway 100.25.5.201  
 Remote Port 4500

- On the secondary device, member information is displayed:



## CLI

Use the `diagnose sys ha autoscale-peers` command to list autoscale member information.

## Support for new VM bandwidth-limited SKUs - 6.4.2

Four new stackable SKUs allow you to purchase and deploy VMs with limited bandwidths per interface. The bandwidth limits are calculated per interface, or aggregate interface, per direction. Management only interfaces are exempt from the limit.

Each SKU includes one of the following service bundles:

- FortiClient only
- UTM
- Enterprise
- 360 Protection

The FortiGate gets the service bundle and bandwidth from FortiGuard after the VM license is uploaded to the FortiGate.

These examples show two of the license options:

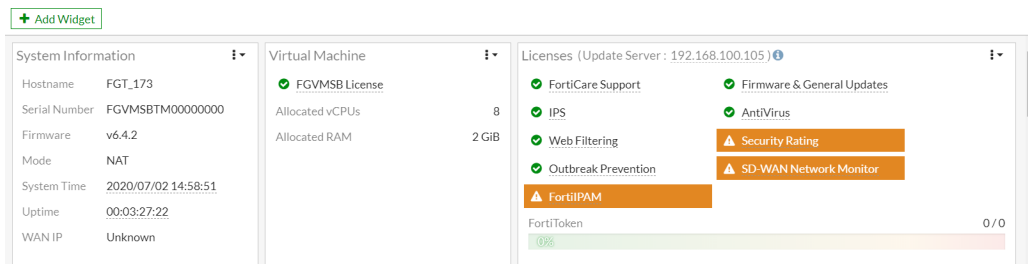
- UTM and 100Gbps bandwidth (unlimited bandwidth)
- 360 Protection with 900Mbps bandwidth



The 360 Protection service bundle has been discontinued.

## UTM and 100Gbps

After the license is imported and validated, FortiGuard services are shown on the *Status* dashboard.



The CLI shows unlimited bandwidth for the license and no bandwidth for interfaces, because it is unlimited.

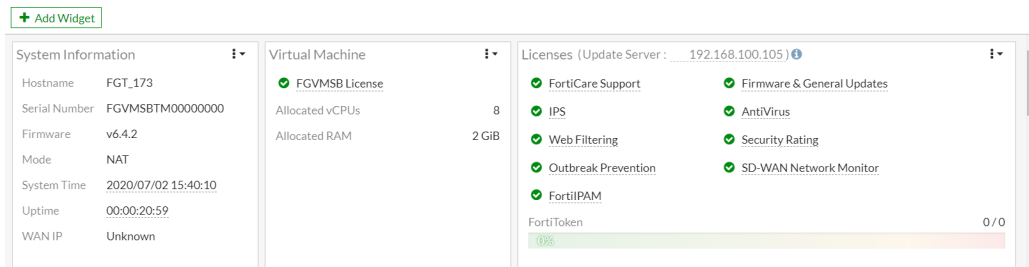
```
# diagnose debug vm-print-license
SerialNumber: FGVMSBTM20090007
CreateDate: Fri May 15 00:36:41 2020
License expires: Sun May 16 17:00:00 2021
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: SB (19)
CPU: 2147483647
MEM: 2147483647
Bandwidth: unlimited

# diagnose netlink interface list port3

if=port3 family=00 type=1 index=5 mtu=1500 link=0 master=0
ref=14 state=start present fw_flags=10008000 flags=up broadcast run multicast
Qdisc=pfifo_fast hw_addr=00:0c:29:15:df:1f broadcast_addr=ff:ff:ff:ff:ff:ff
stat: rxp=857 txp=5 rxb=80456 txb=312 rxe=0 txe=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=14
```

## 360 Protection and 900Mbps bandwidth

After the license is imported and validated, FortiGuard services are shown on the *Status* dashboard.



The CLI shows an extra 10% bandwidth for the license and interfaces, not including management interfaces:

```
# diagnose debug vm-print-license
SerialNumber: FGVMsBTM00000000
CreateDate: Sat May 16 02:27:24 2020
License expires: Mon May 17 17:00:00 2021
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: SB (19)
CPU: 2147483647
MEM: 2147483647
Bandwidth: 990000 kbps

# diagnose netlink interface list port2

if=port2 family=00 type=1 index=4 mtu=1500 link=0 master=0
ref=28 state=start present fw_flags=8000 flags=up broadcast run multicast
Qdisc=pfifo_fast hw_addr=00:0c:29:15:df:15 broadcast_addr=ff:ff:ff:ff:ff:ff
inbandwidth=990000 (kbps)          total_bytes=0    drop_bytes=0
outbandwidth=990000 (kbps)
    priority=0      allocated-bandwidth=10 (kbps)    total_bytes=125K      drop_bytes=0
    priority=1      allocated-bandwidth=0 (kbps)    total_bytes=0         drop_bytes=0
    priority=2      allocated-bandwidth=0 (kbps)    total_bytes=0         drop_bytes=0
    priority=3      allocated-bandwidth=0 (kbps)    total_bytes=864       drop_bytes=0
    priority=4      allocated-bandwidth=989989 (kbps)    total_bytes=0         drop_bytes=0
stat: rxp=490 txp=574 rxb=289785 txb=126227 rx=0 tx=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=28
```

## Aggregate interfaces

Aggregate interfaces have the same bandwidth limit as individual interfaces:

```
config system interface
    edit "agg56"
        set vdom "root"
        set allowaccess ping https ssh http
        set type aggregate
        set member "port5" "port6"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 15
```

```

    next
end

# diagnose netlink interface list agg56

if=agg56 family=00 type=1 index=16 mtu=1500 link=0 master=0
ref=42 state=start present fw_flags=3800 flags=up broadcast master multicast
Qdisc=noqueue hw_addr=00:0c:29:15:df:33 broadcast_addr=ff:ff:ff:ff:ff:ff
inbandwidth=990000 (kbps)          total_bytes=0    drop_bytes=0
outbandwidth=990000 (kbps)
    priority=0      allocated-bandwidth=0 (kbps)      total_bytes=90    drop_bytes=0
    priority=1      allocated-bandwidth=0 (kbps)      total_bytes=0     drop_bytes=0
    priority=2      allocated-bandwidth=0 (kbps)      total_bytes=0     drop_bytes=0
    priority=3      allocated-bandwidth=0 (kbps)      total_bytes=0     drop_bytes=0
    priority=4      allocated-bandwidth=110000 (kbps)  total_bytes=0     drop_bytes=0
stat: rxp=53501934 txp=139 rxb=3210121819 txb=17166 rx=0 tx=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=7 arp_entry=0 refcnt=42

# diagnose netlink interface list port5

if=port5 family=00 type=1 index=7 mtu=1500 link=0 master=16
ref=12 state=start present fw_flags=0 flags=up broadcast run noarp slave multicast
Qdisc=pfifo_fast hw_addr=00:0c:29:15:df:33 broadcast_addr=ff:ff:ff:ff:ff:ff
inbandwidth=990000 (kbps)          total_bytes=0    drop_bytes=0
outbandwidth=990000 (kbps)
    priority=0      allocated-bandwidth=0 (kbps)      total_bytes=8770    drop_bytes=0
    priority=1      allocated-bandwidth=0 (kbps)      total_bytes=0       drop_bytes=0
    priority=2      allocated-bandwidth=0 (kbps)      total_bytes=0       drop_bytes=0
    priority=3      allocated-bandwidth=0 (kbps)      total_bytes=0       drop_bytes=0
    priority=4      allocated-bandwidth=989999 (kbps)  total_bytes=0       drop_bytes=0
stat: rxp=70 txp=71 rxb=9289 txb=8770 rx=0 tx=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=12

# diagnose netlink interface list port6

if=port6 family=00 type=1 index=8 mtu=1500 link=0 master=16
ref=12 state=start present fw_flags=0 flags=up broadcast run noarp slave multicast
Qdisc=pfifo_fast hw_addr=00:0c:29:15:df:33 broadcast_addr=ff:ff:ff:ff:ff:ff
inbandwidth=990000 (kbps)          total_bytes=0    drop_bytes=0
outbandwidth=990000 (kbps)
    priority=0      allocated-bandwidth=0 (kbps)      total_bytes=8770    drop_bytes=0
    priority=1      allocated-bandwidth=0 (kbps)      total_bytes=0       drop_bytes=0
    priority=2      allocated-bandwidth=0 (kbps)      total_bytes=0       drop_bytes=0
    priority=3      allocated-bandwidth=0 (kbps)      total_bytes=0       drop_bytes=0
    priority=4      allocated-bandwidth=989999 (kbps)  total_bytes=0       drop_bytes=0
stat: rxp=54003304 txp=71 rxb=3240198976 txb=8770 rx=0 tx=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=12

```

## Management interfaces

Normal and VPN interfaces that are dedicated to management do not have a bandwidth limitation

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 10.6.30.173 255.255.255.0
        set allowaccess ping https ssh http fgfm
        set type physical
        set dedicated-to management
        set snmp-index 1
    next
end

# diagnose netlink interface list port1

if=port1 family=00 type=1 index=3 mtu=1500 link=0 master=0
ref=18 state=start present fw_flags=0 flags=up broadcast run multicast
Qdisc=pfifo_fast hw_addr=00:0c:29:15:df:0b broadcast_addr=ff:ff:ff:ff:ff:ff
stat: rxp=6957 txp=4270 rxb=1196300 txb=2942486 rx=0 tx=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=18
```

## Setting the interface bandwidth

The in and out bandwidths can be configured with 10% extra bandwidth:

```
config system interface
    edit "port3"
        set vdom "root"
        set ip 172.16.200.173 255.255.255.0
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response
    fabric ftm
        set type physical
        set inbandwidth 990000
        set outbandwidth 990000
        set snmp-index 3
    next
end
```

Setting the bandwidth too high will result in an error:

```
# set inbandwidth 1000000
Should be in the range of 0 - 990000.
node_check_object fail! for outbandwidth 1000000

value parse error before '1000000'
Command fail. Return code -2
```

## FOS support of VM-ELA (FortiFlex) - 6.4.2

FortiFlex is an Enterprise License Agreement for Virtual Machine licensing to help users manage and monitor their VM subscriptions on the FortiCloud portal. Resource consumption is calculated using a point based system.

The program allows a single VM consumption entitlement (corresponding to a license per VM) which contains both VM base and one of four FC/FGD protection services. Resource consumption is calculated based upon certain predefined points that are converted to monetary values on a daily-basis. Customers are not required to have a pair of VM base and FortiCloud service entitlements separately, or order every single entitlement per VM, which is the case for FGT-VM/VMv and S-series.

FortiFlex has two sub programs:

- **Prepaid for Enterprise:** Point pack SKUs are purchased in advance. Points are deducted on a daily basis based on resource consumption. Unused points can be rolled over.
- **Postpaid for MSSP:** Points are calculated based on resource consumption and are billed directly by the Fortinet Finance team. Purchase of a program SKU is required. Neither point pack SKUs nor roll-overs are applicable.

Corresponding SKUs:

- **Flex VM Post\_Paid:** FC-10-ELAVS-221-02-DD
- **Flex VM Pre\_Paid:** FC-10-ELAVR-221-02-DD and LIC-ELAVM-10K

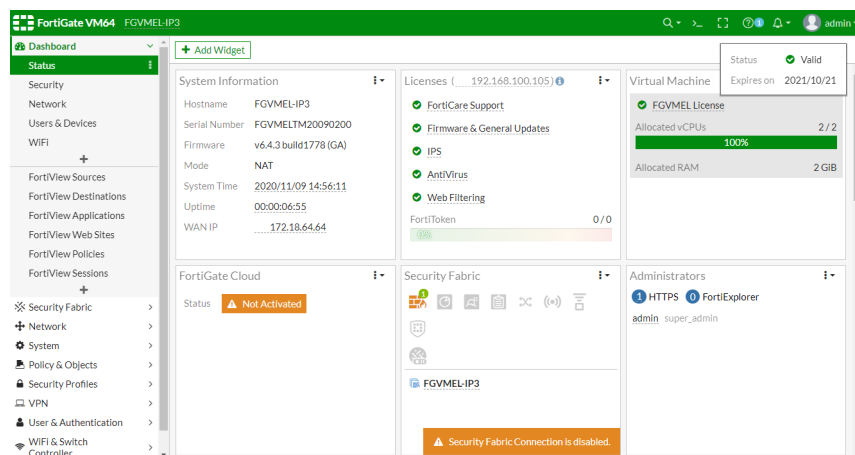
For information about the FortiFlex program, point packages, and deployment, see the following guides in the Fortinet Document Library.

- [FortiFlex Program Guide](#)
- [FortiFlex Deployment Guide](#)

### To view FortiFlex licenses in the GUI:

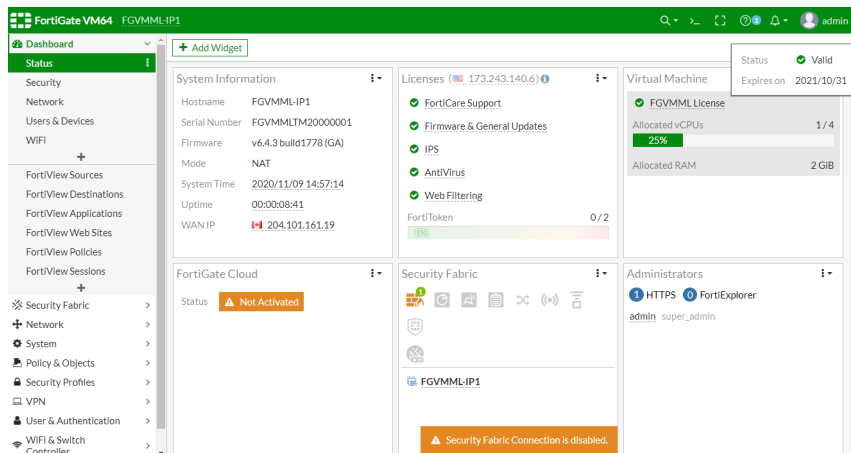
Go to *Dashboard > Status*. The *Virtual Machine* widget displays the FortiFlex license.

The image below shows the FortiFlex post-paid license:



The image below shows the FortiFlex pre-paid license:





## Liveness detection on NSX-T - 6.4.3

Liveness detection can force the Service Insertion datapath not to use a specific VM until its service manager has updated the VM's configuration. This can be required when a new FortiGate VM is deployed and should not reply to liveness detection queries or forward any traffic until it has received the required configuration from the service manager. The Service Insertion platform will instead use an already configured VM, if one is available.

The service can be registered in NSX-T manager using the python tool with the following parameter in the script:

```
"service_capability": {
  "nsh_liveness_support_enabled": True
},
```

When registered, the VM receives pings on its dataplane interface to detect the liveness of the service. If a failure occurs on the VM, NSX-T will take the action specified for the liveness service chain failure policy:

- *Allow* - Send traffic to the destination VM when the service VM fails.
- *Block* - Do not send traffic to the destination VM when the service VM fails.

See the [VMware NSX-T documentation](#) for more information. This feature is supported for NSX-T 2.5 and 3.0.

## Add FIPS cipher mode for AWS and Azure FortiGate VMs - 6.4.3

In `fips-ciphers` mode, only a restricted set of ciphers are allowed for features requiring encryption such as SSH, IPsec, IKE/IPsec, SSL VPN, and HTTPS. Other unsecure protocols such as Telnet, TFTP and HTTP access to the cloud FortiGate-VM are not allowed.



Before enabling `fips-ciphers` mode, remove any existing IPsec configurations.

### To enable FIPS cipher mode:

```
config system fips-cc
  set status fips-ciphers
```

end

The following behavior occurs when FIPS cipher mode is enabled:

- A license, image, configuration, and so on can be restored from an FTP server.
- The following options are available:

<b>SSH algorithms</b>	<ul style="list-style-type: none"> <li>• aes128-gcm@openssh.com</li> <li>• aes256-gcm@openssh.com</li> <li>• hmac-sha2-256</li> <li>• hmac-sha2-512</li> </ul>
<b>IKE/IPsec phase1 proposals</b>	<ul style="list-style-type: none"> <li>• aes128gcm-prfsha256</li> <li>• aes128gcm-prfsha384</li> <li>• aes128gcm-prfsha512</li> <li>• aes256gcm-prfsha256</li> <li>• aes256gcm-prfsha384</li> <li>• aes256gcm-prfsha512</li> </ul>
<b>IKE/IPsec phase2 proposals</b>	<ul style="list-style-type: none"> <li>• aes128gcm</li> <li>• aes256gcm</li> </ul>
<b>IKE/IPsec DH groups</b>	<ul style="list-style-type: none"> <li>• Default = 19, or any three from 14 - 21, 27 - 32</li> </ul>
<b>HTTPS for admin and SSL VPN (with RSA server certificate) TLS suites</b>	<p>PFS:</p> <ul style="list-style-type: none"> <li>• TLS_AES_256_GCM_SHA384</li> <li>• ECDHE-RSA-AES256-GCM-SHA384</li> <li>• DHE-RSA-AES256-GCM-SHA384</li> <li>• TLS_AES_128_GCM_SHA256</li> <li>• ECDHE-RSA-AES128-GCM-SHA256</li> <li>• DHE-RSA-AES128-GCM-SHA256</li> </ul> <p>Elliptic curves:</p> <ul style="list-style-type: none"> <li>• prime256v1</li> <li>• secp384r1</li> <li>• secp521r1</li> </ul> <p>DH group:</p> <ul style="list-style-type: none"> <li>• RFC3526/Oakley group 14 (2048 bits)</li> </ul>
<b>HTTPS for admin and SSL VPN (with ECC server certificate) TLS suites</b>	<p>PFS:</p> <ul style="list-style-type: none"> <li>• TLS_AES_256_GCM_SHA384</li> <li>• ECDHE-ECDSA-AES256-GCM-SHA384</li> <li>• TLS_AES_128_GCM_SHA256</li> <li>• ECDHE-ECDSA-AES128-GCM-SHA256</li> </ul> <p>Elliptic curves:</p> <ul style="list-style-type: none"> <li>• prime256v1</li> <li>• secp384r1</li> <li>• secp521r1</li> </ul>

- The FortiCare license is validated.

- FortiGuard databases and engines are updated.
- The DH-RSA-AES128-GCM-SHA256 and DH-RSA-AES256-GCM-SHA384 ciphers are not supported.
- A factory reset is required to disable `fips-ciphers` mode.

## IMDSv2 for FortiGate-VM on AWS - 6.4.3

FortiGate-VM on AWS uses Amazon EC2 Instance Metadata Service version 2 (IMDSv2) to query and retrieve metadata from AWS cloud.

IMDSv2 provides enhanced security to protect against open WAF, open reverse proxies, SSRF vulnerabilities, and open L3 firewalls and NATs.

## Add VDOM support for NSX-T - 6.4.3

By configuring the service chain and service index, NSX-T east-west traffic can be redirected to a designated FortiGate VDOM.

The following commands have been added:

```
config nsxt setting
    set liveness {enable | disable}
    set service <service name>
end

config nsxt service-chain
    edit <ID>
        set name <chain name>
        config service-index
            edit <forward index>
                set reverse-index <integer>
                set name <index name>
                set vd <VDOM>
            next
        end
    next
end
```

Where:

reverse-index <integer>	Value from (1 - 255, default = 1).
-------------------------	------------------------------------



After upgrading, the `nsxt setting` and `nsxt service-chain` are automatically configured and redirect traffic to the root VDOM.

### To redirect traffic from the root to the vd1 VDOM:

1. Enable liveness detection:

```
(global) # config nsxt setting
    set liveness enable
end
```

## 2. Configure the service chain and service index:

```
(global) # config nsxt service-chain
    edit 1
        config service-index
            edit 1
                set vd "vd1"
            next
        end
    next
end
```

## 3. Configure the GENEVE interface linked with port2:

```
(vd1) #config system geneve
    edit "vd1-int"
        set interface "port2"
        set vni 1
        set remote-ip 10.0.0.1
    next
    edit "vd1-ext"
        set interface "port2"
        set vni 2
        set remote-ip 10.0.0.1
    next
end
```

## 4. Configure the GENEVE interface as a virtual wire pair:

```
(vd1) #config system virtual-wire-pair
    edit "1"
        set member "vd1-int" "vd1-ext"
    next
end
```

## 5. Configure the firewall policy:

```
(vd1) # config firewall policy
    edit 1
        set srcintf "vd1-int" "vd1-ext"
        set dstintf "vd1-int" "vd1-ext"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set ssl-ssh-profile "certificate-inspection"
        set logtraffic all
        set capture-packet enable
        set auto-asic-offload disable
    next
end
```

**6. Verify the traffic:**

```
(vd1) # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
1.088228 vd1-int in 172.16.10.92 -> 172.16.20.94: icmp: echo request
1.088244 vd1-ext out 172.16.10.92 -> 172.16.20.94: icmp: echo request
1.088618 vd1-ext in 172.16.10.92 -> 172.16.20.94: icmp: echo request
1.088626 vd1-int out 172.16.10.92 -> 172.16.20.94: icmp: echo request
```

**Support OCI compute shapes that use Mellanox network cards - 6.4.3**

Support has been added to deploy FortiGate VMs that are paravirtualized with SR-IOV and DPDK/vNP on OCI shapes that use Mellanox network cards.

**To deploy the VM using a Mellanox card:**

1. Create an instance using a compute shape that supports the Mellanox network card, such as VM.Standard.E3.Flex.
2. In the OCI console, verify the instance has SR-IOV enabled:

```
# oci compute instance get --instance-id <instance ID>
{
  "data": {
    ...
    "launch-mode": "PARAVIRTUALIZED",
    "launch-options": {
      "boot-volume-type": "PARAVIRTUALIZED",
      "firmware": "BIOS",
      "is-consistent-volume-naming-enabled": false,
      "is-pv-encryption-in-transit-enabled": false,
      "network-type": "VFIO",
      "remote-data-volume-type": "PARAVIRTUALIZED"
    },
    ...
  },
  ...
}
```

The network type is VFIO (as opposed to PARAVIRTUALIZED), which means that SR-IOV is enabled.

3. In FortiOS, verify that the boot is successful and check instance details:

```
# get system status
Version: FortiGate-VM64-OPC v6.4.3,build1776,201013 (interim)
...
Serial-Number: FGVMULTM20000xxx
IPS Malicious URL Database: 2.00798(2020-10-15 09:20)
License Status: Valid
License Expiration Date: 2021-07-01
VM Resources: 2 CPU, 16085 MB RAM
VM Instance ID: ocid1.instance.oc1.iad.xxxxxxxx
...
```

4. Check the NIC driver to ensure that it is mlx5\_core:

```
# diagnose hardware deviceinfo nic port1
Name:          port1
Driver:        mlx5_core
...
```

**5. Enable DPDK:**

```
config dpdk global
    set status enable
    set interface port2 port1
end
```

**6. Reboot the FortiGate.****7. Verify the drivers are now net\_mlx5 to signify they are DPDK enabled:**

```
# diagnose hardware deviceinfo nic port1
Name:          port1
Driver:        net_mlx5
...
```

**8. Verify that DPDK was initiated successfully:**

```
# diagnose dpdk log show early-init
-----
DPDK early initialization starts at 2020-10-16 00:37:36(UTC)
-----
Content of early configuration file:
    status=1
    multiqueue=0
    sleep-on-idle=0
    elasticbuffer=0
    per-session-accounting=1
    hugepage-percentage=30
    nr_hugepages=2412
    interfaces=port1 port2
    cpus=0 1
    rxcpus=0 1
    vnpcpus=0 1
    ipscpus=0 1
    txcpus=0 1
Parse config file success!

Check CPU definitions 'cpus'
Check CPU definitions 'rxcpus'
Check CPU definitions 'ipscpus'
Check CPU definitions 'vnpcpus'
Check CPU definitions 'txcpus'
Check CPUs success!

Huge page allocation done

Ports enabled for DPDK:
    port1
    port2
Port name to device name mapping:
    port1: eth0
    port2: eth1
    port3: eth2
    port4: eth3
    ...

Start enabling DPDK kernel driver for port 'port1'...
Getting PCI device info for eth0...
```

```
reading pci dev /sys/class/net/eth0
link path: ../../devices/pci0000:00/0000:00:03.0/net/eth0
Device info of eth0:
    dev_name: eth0
    macaddr: 00:00:17:02:3c:d9
    pci_vendor: 0x15b3
    pci_device: 0x101a
    pci_id: 0000:00:03.0
    pci_domain: 0
    pci_bus: 0
    pci_devid: 3
    pci_function: 0
    guid: n/a
Device eth0 is mlx5_core name changed to slv0
Creating DPDK kernel driver for device eth0...
Add VNP dev: eth0 PCI: 0000:00:03.0, Succeeded
DPDK kernel driver for eth0 successfully created
DPDK kernel driver enabled for port 'port1' (device name 'eth0')

Start enabling DPDK kernel driver for port 'port2'...
Getting PCI device info for eth1...
reading pci dev /sys/class/net/eth1
link path: ../../devices/pci0000:00/0000:00:05.0/net/eth1
Device info of eth1:
    dev_name: eth1
    macaddr: 02:00:17:02:bd:df
    pci_vendor: 0x15b3
    pci_device: 0x101a
    pci_id: 0000:00:05.0
    pci_domain: 0
    pci_bus: 0
    pci_devid: 5
    pci_function: 0
    guid: n/a
Device eth1 is mlx5_core name changed to slv1
Creating DPDK kernel driver for device eth1...
Add VNP dev: eth1 PCI: 0000:00:05.0, Succeeded
DPDK kernel driver for eth1 successfully created
DPDK kernel driver enabled for port 'port2' (device name 'eth1')
Bind ports success!

Make UIO nodes success!

DPDK sanity test passed
```

**9. Send traffic through the FortiGate and verify the statistics to ensure packets are actually passing through DPDK:**

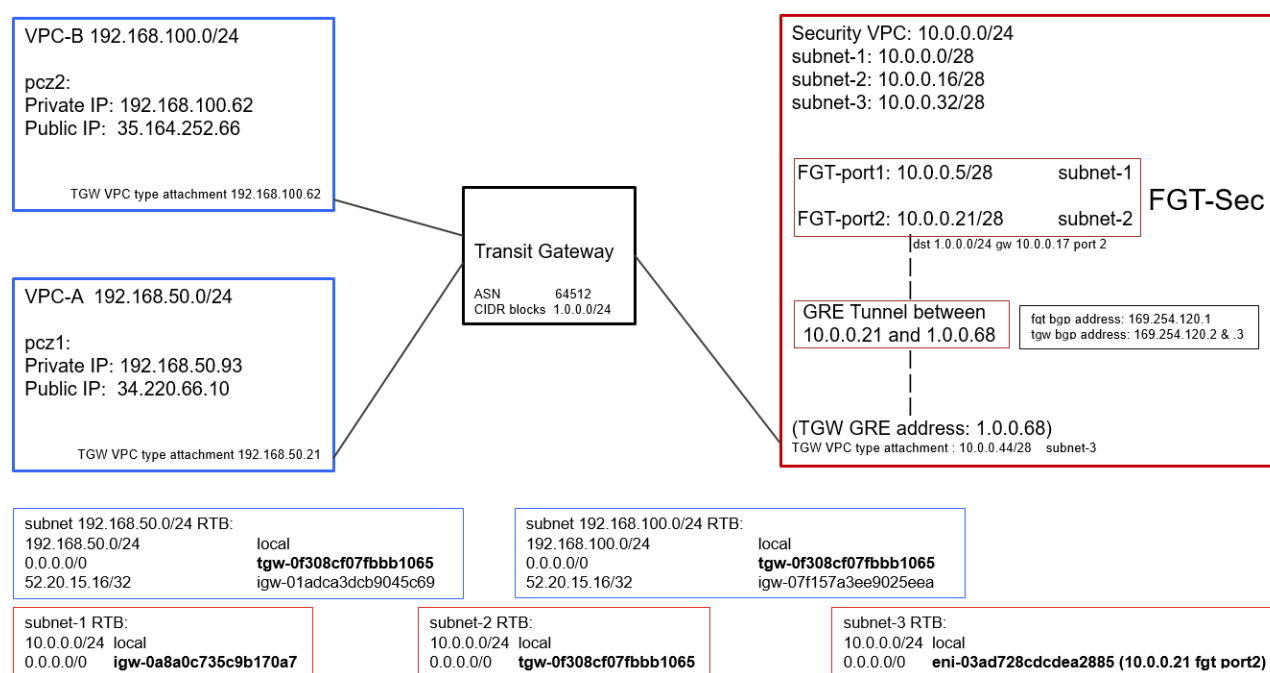
```
# diagnose dpdk statistics show engine
# diagnose dpdk statistics show port
# diagnose dpdk statistics show vnp
# diagnose dpdk statistics show memory
```

## Support AWS transit gateway connect attachment and connect peer - 6.4.3

AWS's transit gateway (TGW) connect attachment and connect peer are components for a new way of building a connection between the TGW and a transit VPC using a GRE tunnel overlay. When building a transit VPC that FortiGates are securing, the TGW connect attachment forms a GRE tunnel between the FortiGate-VM and the TGW. This deployment uses border gateway protocol routing, and a default route is advertised from the FortiGate-VM to the TGW peer. Virtual private clouds (VPC) which must be routed to the FortiGate TGW form VPC connect attachments with the TGW, and route traffic through it.

TGW plugin provides a tighter and a more native integration between the partner gateway appliances and TGW via tunnel attachment. TGW plugin supports GRE-based tunnel attachments, which provide higher performance than IPsec connections, which are currently used for the same purpose. Native GRE-based tunnel attachments support triple the bandwidth as IPsec.

The following shows the example topology:



### To configure the components in AWS:

#### 1. Create a TGW:

- In the AWS management console, go to *VPC > Transit Gateways > Transit Gateways*, then click *Create new*.
- In the *Amazon side ASN* field, enter the AS that the TGW will use. The TGW uses BGP to exchange routes with the FortiGate.
- In the *CIDR* field, specify a CIDR. The connect feature has GRE endpoints on the TGW end, which require a CIDR. You can specify this while creating a TGW as shown, or editing an existing TGW to specify the CIDR.
- Leave other fields as-is.
- Click *Create Transit Gateway*. This example configures the default 64512 as the AS and 1.0.0.0/24 for the CIDR blocks.

- The Security and App VPCs need the transport VPC attachments. For the App VPCs, you can create it in one of the App subnets or on a dedicated subnet. For the Security VPC, since there are two FortiGate-VMs in two AZs, you must create an attachment for each AZ. The architecture includes a dedicated subnet in each AZ for TGW creation.



Create VPC attachments:

- a. Go to *VPC > Transit Gateways > Transit Gateway Attachments*, then click *Create new*.
  - b. From the *Attachment type* dropdown list, select *VPC*.
  - c. In *Subnet IDs*, select the two dedicated subnets for TGW landing.
  - d. Click *Create attachment*.
3. Create the connect attachment. A connect attachment supports the GRE tunnel protocol for high performance and BGP for dynamic routing. After you create a connect attachment, you can create one or more GRE tunnels (also referred to as TGW connect peers) on the connect attachment to connect the TGW and the FortiGate:
- a. Go to *VPC > Transit Gateways > Transit Gateway Attachments*, then click *Create new*.
  - b. From the *Attachment type* dropdown list, select *Connect*.
  - c. From the *Transport Attachment ID* dropdown list, select the attachment that you created in step 2. Since you selected the subnets when creating the attachments in step 2, you cannot select subnets here.
  - d. Click *Create attachment*.
4. Connect peers are the combination of GRE and BGP configuration between the FortiGates and in the Security VPC and the TGW. Create a connect peer:
- a. Go to *VPC > Transit Gateways > Transit Gateway Attachments*, then click the connect attachment that you created in step 3.
  - b. Configure the connect peer between the TGW and the FortiGate-VM in AZ1:
    - i. On the *Connect peers* tab, click *Create Connect peer*.
    - ii. The TGW GRE address is autogenerated. In this example, this value is 1.0.0.68.
    - iii. In the *Peer GRE address* field, enter the interface IP address of the FortiGate-VM where the GRE tunnel will terminate. This example uses 10.0.0.21.
    - iv. In the *Peer ASN* field, enter the AS number that the FortiGate-VM will use. eBGP will be used. Click *Create*.
  - c. Repeat step b to create the connect peer for the FortiGate-VM in AZ2, using the interface IP address and AS number for this FortiGate-VM. After configuring both connect peers, the tunnel status is down as the FortiGate-VMs are not configured for GRE and BGP yet.
5. In this example, all three VPCs connect to the same TGW route table. All three VPCs propagate to the same route table. Inspecting the traffic between the App VPCs would require multiple TGW route tables. Create a TGW route table:
- a. Go to *VPC > Transit Gateways > Transit Gateway Route Table*, then click *Create new*.
  - b. On the *Associations* tab, click *Create association*. Add the attachments that you created in step 2. AWS automatically creates an association with the Security VPC connect attachment that you created in step 3.
  - c. On the *Propagations* tab, click *Create propagation*. Create propagations for the three attachments that you created in step 2 and 3.

### To configure this feature in FortiOS:

These instructions configure the following firewall policies:

- A policy for Internet traffic from application VPCs
- A policy for east-west traffic between application VPCs
- A policy for virtual IP address traffic to application PCs

```
config system gre-tunnel
  edit "tgwc"
    set interface "port2"
    set remote-gw 1.0.0.68
    set local-gw 10.0.0.21
  next
```

```
end
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh fgfm
    next
    edit "port2"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh snmp http telnet
    next
edit "tgwc"
    set vdom "root"
    set ip 169.254.120.1 255.255.255.255
    set allowaccess ping https ssh snmp http
    set type tunnel
    set remote-ip 169.254.120.2 255.255.255.248
    set snmp-index 5
    set interface "port2"
    next
end
config router static
    edit 10
        set dst 1.0.0.0 255.255.255.0
        set gateway 10.0.0.17
        set device "port2"
    next
end
config router bgp
    set as 7115
    set router-id 169.254.101.1
    config neighbor
        edit "169.254.120.2"
            set capability-default-originate enable
            set ebgp-enforce-multihop enable
            set soft-reconfiguration enable
            set remote-as 64512
        next
        edit "169.254.120.3"
            set capability-default-originate enable
            set ebgp-enforce-multihop enable
            set soft-reconfiguration enable
            set remote-as 64512
        next
    next
end
.....
end
config firewall policy
    edit 1
        set srcintf "tgwc"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
```

```

        set service "ALL"
        set nat enable
    next
    edit 2
        set srcintf "tgwc"
        set dstintf "tgwc"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 100
        set srcintf "port1"
        set dstintf "tgwc"
        set srcaddr "all"
        set dstaddr "ec2ssh"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

```

### To verify the configuration:

#### 1. Verify Internet traffic from the Application PC in VPC A:

```

ping 8.8.8.8 -c 1
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=89 time=10.5 ms

diagnose sniffer packet any icmp 4
5.948458 tgwc in 192.168.50.93 -> 8.8.8.8: icmp: echo request
5.948491 port1 out 10.0.0.5 -> 8.8.8.8: icmp: echo request
5.957798 port1 in 8.8.8.8 -> 10.0.0.5: icmp: echo reply
5.957814 tgwc out 8.8.8.8 -> 192.168.50.93: icmp: echo reply

```

#### 2. Verify Internet traffic from the Application PC in VPC B:

```

ping 8.8.8.8 -c 1
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=89 time=10.7 ms

diagnose sniffer packet any icmp 4
1.929761 tgwc in 192.168.100.62 -> 8.8.8.8: icmp: echo request
1.929806 port1 out 10.0.0.5 -> 8.8.8.8: icmp: echo request
1.939127 port1 in 8.8.8.8 -> 10.0.0.5: icmp: echo reply
1.939143 tgwc out 8.8.8.8 -> 192.168.100.62: icmp: echo reply

```

#### 3. Verify east-west traffic between the Application PCs in VPCs A and B:

```

ping 192.168.100.62 -c 1
PING 192.168.100.62 (192.168.100.62) 56(84) bytes of data.

```

```
64 bytes from 192.168.100.62: icmp_seq=1 ttl=252 time=3.34 ms
```

```
diagnose sniffer packet any icmp 4
2.218833 tgwc in 192.168.50.93 -> 192.168.100.62: icmp: echo request
2.218874 tgwc out 192.168.50.93 -> 192.168.100.62: icmp: echo request
2.220736 tgwc in 192.168.100.62 -> 192.168.50.93: icmp: echo reply
2.220746 tgwc out 192.168.100.62 -> 192.168.50.93: icmp: echo reply
```

4. Verify SSH VIP traffic to the Application PC in VPC B. Note that 44.242.126.40 is the FortiGate elastic IP address on port1:

```
ssh -i xxxx ec2-user@44.242.126.40 -p 2222
```

```
Last login: Fri Apr 9 00:12:18 2021 from 169.254.120.1
```

```
__| __|_ )
_| ( / Amazon Linux 2 AMI
___|\___|___|
```

```
diagnose sniffer packet any 'host 192.168.100.62 and port 22' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 192.168.100.62 and port 22]
4.904145 tgwc out 169.254.120.1.47876 -> 192.168.100.62.22: syn 1737745616
4.905891 tgwc in 192.168.100.62.22 -> 169.254.120.1.47876: syn 1376689826 ack
1737745617
4.919022 tgwc out 169.254.120.1.47876 -> 192.168.100.62.22: ack 1376689827
4.919033 tgwc out 169.254.120.1.47876 -> 192.168.100.62.22: psh 1737745617 ack
1376689827
4.920199 tgwc in 192.168.100.62.22 -> 169.254.120.1.47876: ack 1737745658
```

## Support OCI IMDSv2 - 6.4.4

Support was added for OCI IMDSv2, which offers increased security for accessing instance metadata compared to IMDSv1. IMDSv2 is used in OCI SDN connectors and on instance deployments with bootstrap metadata. When upgrading from previous FortiOS builds with legacy IMDSv1 endpoints, the endpoints will be updated to IMDSv2, and the same calls can be made.

The following use cases illustrate IMDSv2 support on the FortiGate-VM.

### To configure the Oracle OCI instance to use IMDSv2:

1. In OCI, deploy an instance using IMDSv2 with bootstrap metadata. There are two methods to enable IMDSv2 :
  - Use the OCI command line to deploy an instance using `user-data`. This example uses a MIME file that contains the license and configuration, as well as a JSON file that specifies to disable V1 metadata.

```
oci compute instance launch
--availability-domain ww1:US-ASHBURN-AD-1
--compartment-id
ocidl.tenancy.oc1..aaaaaaaaaaaa3aaaaaaaaaaaaaaaaa7xxxxxx54aaaaaa4xxxxxxxx55xxxa
--display-name fos-byol-v6.4.6-b2290-emulated
--image-id
```

```

ocidl.image.oc1.iad.aaaaaaa6xxx43xxxxxxxx7aaaaaaaaaaaaaaaaaaaaa3xxxxxxxxxxxxxx
--subnet-id
ocidl.subnet.oc1.iad.aaaaaaa2xxxxxxxxxxxxxxxxxxxxxxxx5aaa4xxxxxxxxxxxx42aaa
--shape VM.Standard1.4
--assign-public-ip true
--user-data-file /home/oci/userdata/mime.txt
--ssh-authorized-keys-file /home/oci/userdata/myfirstkeypair.pub
--instance-options file://home/oci/scripts/metadatav2.json

root@mail:/home/oci/scripts# cat metadatav2.json
{
  "areLegacyImdsEndpointsDisabled": true
}

```

- While the instance is running, edit the instance metadata service version in the GUI ,and change the allowed IMDS version to **VERSION 2 ONLY** (see [Getting Instance Metadata](#) in the OCI documentation).

Edit Instance Metadata Service Version [Help](#) [Close](#)

When enabled, applications that rely on the [instance metadata service \(IMDS\)](#) must use the IMDSv2 endpoint and provide an authorization header. All requests to IMDSv1 are denied. Enable this setting only if the image supports IMDSv2.

ALLOWED IMDS VERSION

☐ VERSION 1 AND VERSION 2  
Allows requests to IMDSv1 and IMDSv2 to succeed. This setting is backwards compatible.

☒ VERSION 2 ONLY  
Denies all requests to the IMDSv1 endpoint. All requests must use the IMDSv2 endpoint and provide an authorization header. Enable this setting only if the image supports IMDSv2.

[Save Changes](#) [Cancel](#)

2. The FortiGate will use the metadata v2 endpoints to get the metadata bootstrap information. In FortiOS, verify this by running the following after bootup:

```
# diagnose debug cloudinit show
```

**To configure an SDN connector with meta-IAM enabled and firewall addresses to obtain dynamic addresses:**

1. Configure an IAM policy and dynamic group (see [How Policies Work](#) and [Managing Dynamic Groups](#) in the OCI documentation).

Identity > Policies > Policy Detail

**thomasscriptpolicy**

[Edit Policy](#) [Add Tags](#) [Delete](#)

**Policy Information** **Tags**

OCID: [Show](#) [Copy](#)

Version Date: Keep version current

Compartment: fortinetoracled1 (root)

Description: policy for sdn-connector

Created: Wed, Nov 18, 2020, 00:45:21 UTC

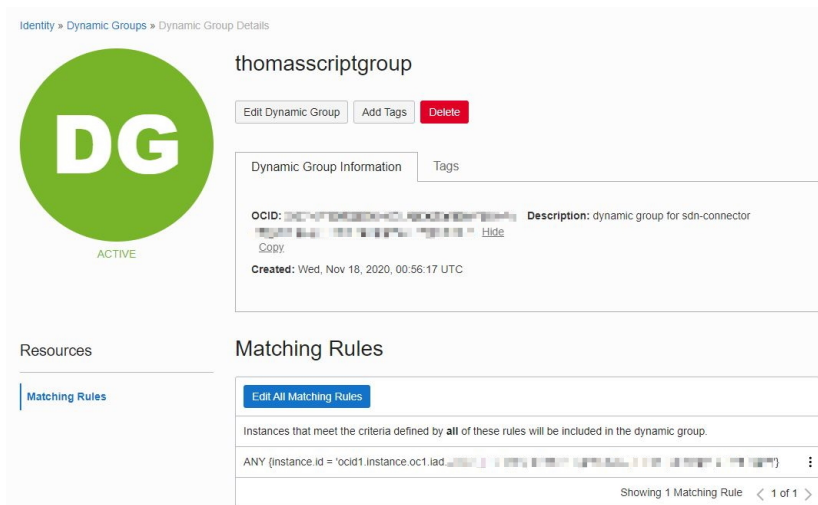
**Resources**

[Statements](#)

[Edit Policy Statements](#)

Allow dynamic-group thomasscriptgroup to manage all-resources in TENANCY

Showing 1 item



2. In FortiOS, configure the OCI Fabric connector (see [OCI SDN connector](#) for detailed instructions):
  - a. Create the SDN connector.
  - b. Verify that the OCI connector comes up (*Security Fabric > External Connectors* page indicates the status is up).
  - c. Configure a dynamic firewall address with a filter.
  - d. Verify the dynamic firewall address is resolved by the SDN connector.

#### To manually update the external IP:

```
# execute update-eip
instance: fos-byol-v6.4.6-b2290-emulated
  vn1c0: fos-byol-v6.4.6-b2290-emulated
    10.0.0.58 (129.213.138.192)
port1: 10.0.0.58, eip: 129.213.138.192
EIP is updated successfully
```

#### To verify the OCI daemon debugs related to metadata:

```
# diagnose test application ocid 4
instance: fos-byol-v6.4.6-b2290-emulated
  vn1c0: fos-byol-v6.4.6-b2290-emulated
    10.0.0.58

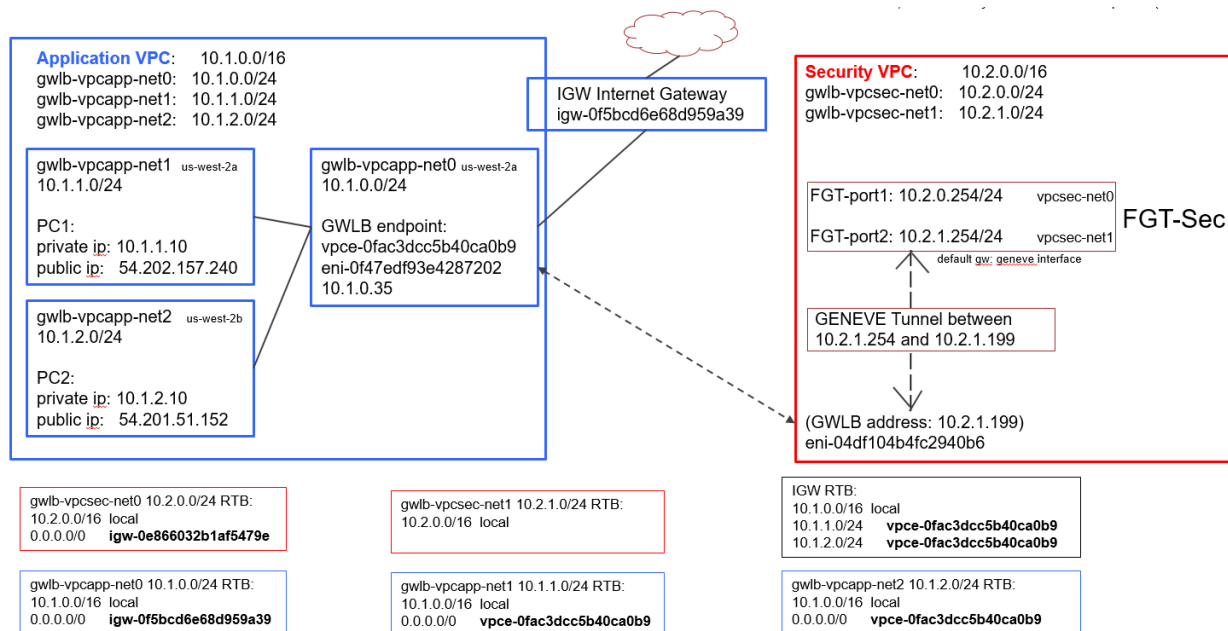
# diagnose test application ocid 5
Compartment
Id:ocid1.tenancy.oc1..aaaaaaaa3aaaaaaaaaaaaaaaa7xxxxxx54aaaaaa4xxxxxxxx55xxxa
Instance Id:ocid1.instance.oc1.iad.aaaaaaaaaaaaaaaa4aaaaa5aaaaaaaa4xxxxxxxx2aaaaaaaa
Instance Name:fos-byol-v6.4.6-b2290-emulated
OCI Regarxiehlion:us-ashburn-1

# diagnose test application ocid 6
Instance Principal Token has been refreshed
```

## GENEVE support for AWS gateway load balancer - 6.4.4

This enhancement adds support for the AWS generic networking for virtual environments (GENEVE) protocol in FortiOS. GENEVE provides a "bump in the wire" service, which diverts traffic within a virtual private cloud (VPC) to an appliance or cluster of appliances. The gateway load balancer (GWLB) accomplishes this by combining L3 gateway and L4 LB features. Users direct VPC route tables to the GWLB, which forwards traffic to a service, such as a web application firewall or next generation firewall. This feature is critical to support, as a table stakes routing feature within AWS for individual deployments, multitenant use cases, autoscaling, and other deployment scenarios for north-south and east-west traffic flows. It also removes the need to use SNAT in many scenarios.

To configure this feature, you must create a GWLB on AWS, configure the related subnet routing table, and add the FortiGate interface IP address as a GWLB-registered target. The following instructions assume that you have configured the GWLB environment in AWS based on the topology:



Creating one GWLB per zone is recommended.

### To configure FortiOS for GENEVE support:

#### 1. Configure the GENEVE interface:

```
config system geneve
  edit "g1"
    set interface "port2"
    set type ppp
    set remote-ip 10.2.1.199
  next
end
```

#### 2. Configure a static route and firewall policy:

```
config router static
  edit 1
```

```

        set device "g1"
    next
end
config firewall policy
    edit 1
        set srcintf "g1"
        set dstintf "g1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end

```

### 3. Ensure that FortiGate can handle the traffic.

#### a. From PC1, ping PC2:

```

root@CtrlPC-1:~# ping 54.201.51.152 -c 1
PING 54.201.51.152 (54.201.51.152) 56(84) bytes of data.
64 bytes from 54.201.51.152: icmp_seq=1 ttl=223 time=14.7 ms

```

#### b. Perform a sniffer trace to determine if packets are traveling the expected route:

```

FGT-GWLB-1 (FG-traffic) # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
1.558522 g1 in 204.101.161.19 -> 10.1.2.10: icmp: echo request
1.558560 g1 out 204.101.161.19 -> 10.1.2.10: icmp: echo request
1.560286 g1 in 10.1.2.10 -> 204.101.161.19: icmp: echo reply
1.560294 g1 out 10.1.2.10 -> 204.101.161.19: icmp: echo reply

FGT-GWLB-1 (FG-traffic) # diagnose sniffer packet port2 'port 6081'
Using Original Sniffing Mode
interfaces=[port2]
filters=[port 6081]
1.029128 10.2.1.199.60004 -> 10.2.1.254.6081: udp 80
1.029157 10.2.1.254.60004 -> 10.2.1.199.6081: udp 80
1.037826 10.2.1.199.60004 -> 10.2.1.254.6081: udp 264
1.037841 10.2.1.254.60004 -> 10.2.1.199.6081: udp 264

```

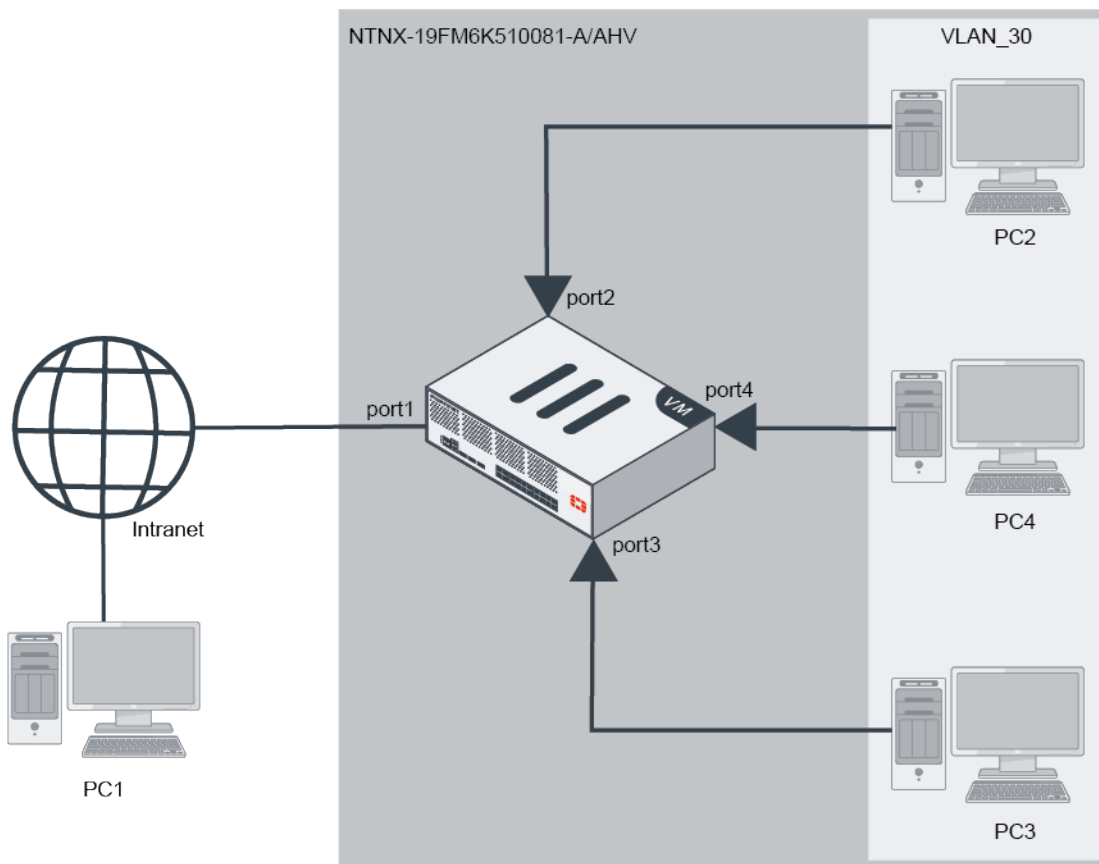
## Nutanix service chaining - 6.4.5

FortiOS supports Nutanix service chaining to allow a service chain to direct network traffic to the FortiGate-VM for scanning. This requires the Calm and Flow features to be enabled on Nutanix, and for Prism Central to be installed on the Nutanix Acropolis hypervisor (AHV).

Nutanix service chains define a set of network function VMs (NFV) for advanced traffic processing. You can direct each defined flow in an application policy through a service chain when a chain exists. For examples, the service chain can direct network traffic on a specific port to a VM for antivirus scanning, deep packet, inspection, or packet capture. You can combine NFVs in a chain to apply multiple functions to guest VM traffic.

The following shows an example topology for this feature:





The following describes the topology in this example:

- The Nutanix AHV has Prism Central installed, with Calm and Flow enabled.
- There are three Ubuntu VMs (PC2, PC3, and PC4) installed to AHV and connected to vlan30.
- The FortiGate-VM has the following interfaces attached:
  - One management interface
  - Three network function chain interfaces

With this topology, you can test whether the feature is functioning by directing traffic between PC2 and PC3 through the FortiGate's virtual wire pair port2-port3 interfaces by the Nutanix service chain feature.

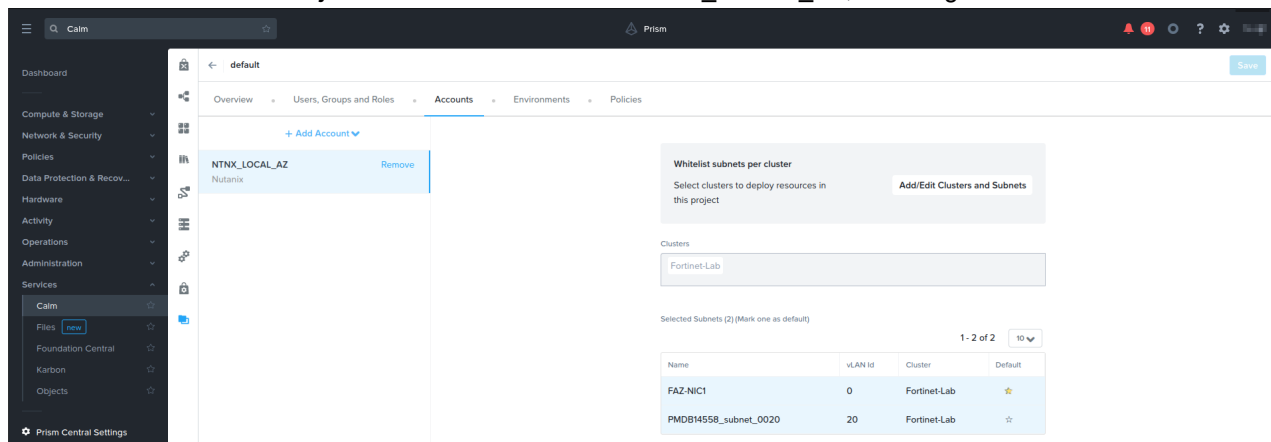
The following instructions describe how to configure the deployment that the topology diagram shows. Substitute the values from your own deployment where necessary.

These deployment instructions were tested using the following Nutanix platform details:

- Prism Central pc.2021.9.0.2
- Acropolis operating system 5.20.1.1
- Calm 3.3.0
- Cluster Maintenance Utilities 1.0.0.
- Epsilon 3.3.0
- Flow Security 1.0.0
- Licensing LM.2021.2.1
- NCC 4.3.0

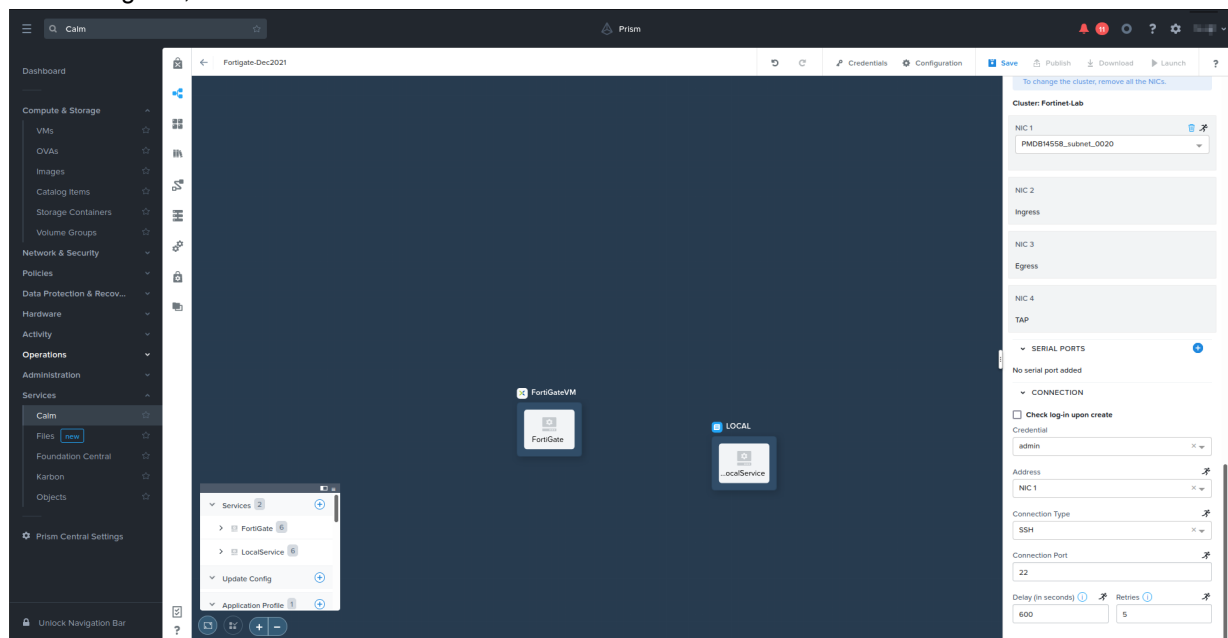
## To deploy the FortiGate-VM to the Nutanix cluster using the Calm blueprint:

1. Sign in to Prism Central.
2. Go to *Compute & Storage > Images*. Click *Import Images*, and upload the fortios.qcow2 image.
3. Go to *Services > Calm > Projects*. Add a user account to NTN\_X\_LOCAL\_AZ, selecting a default subnet.



4. Upload and configure the JSON file:
  - a. Go to *Blueprint*. Upload the JSON file. In this example, it is Fortigate-Dec2021.json file.
  - b. Go to *Credentials*, and set a password for the admin user. Save.
  - c. Click the AHV application profile and configure it as follows:
    - i. For *NF\_CHAIN\_NAME*, enter the desired chain name. In this example, it is FORTIGATE\_CHAIN.
    - ii. For *CLUSTER\_NAME*, enter the desired cluster name. In this example, it is Fortinet-Lab.
    - iii. For *PC\_IP*, enter the PC IP address. In this example, it is 192.168.20.58.
5. Click *Services, Fortigate* to configure the VM name, operating system image, and network adapters:
  - a. You will use a cloud-init script to configure the FortiGate-VM. Enable *Guest Customization*, and select *Cloud-init*. Enter the desired script.
  - b. Under *Disks*, from the *Operation* dropdown list, select *Clone from Image Service*.
  - c. From the *Image* dropdown list, select the fortios.qcow2 image.
  - d. Connect NIC1 to the management subnet, and add three network function chain interfaces: NIC2 for ingress,

NIC2 for egress, and NIC4 for TAP.



6. Click **Save**.
7. Click **Launch**. In the *Application Name* field, enter the desired name to deploy the blueprint. In this example, it is Fortigate-BP.
8. Confirm that the resources were successfully deployed:
  - a. Go to *Services > Calm > Applications*, and click the application name. In this example, it is Fortigate-BP.
  - b. On the *Audit* tab, check the process status. The process may take ten to fifteen minutes. If an *IP not found error* occurs, disregard it. You can configure the port1 static IP address later through FortiGate-VM console access.
  - c. On the *Overview* tab, check the application summary.
  - d. Go to *Administration > Categories*. Verify that the network\_function\_provider FORTIGATE\_CHAIN was created.
9. Go to *Compute & Storage > VMs*. On the *List* tab, verify that the FortiGate-VM was deployed to AHV as NFVM. Select it, then select **Launch console**.

## To direct traffic through the FortiGate-VM:

1. In Prism Central, go to *Categories > AppTier*. Click *Update*. Add FT-Client and FT-Server, then save.

Update Category

---

**General**

Name ⓘ

AppTier

Category cannot be renamed as it is in use by one or more policies.

Purpose ⓘ

Application tier.

---

**Values** ⓘ

System defined values cannot be updated or removed

Default	Unused	-
FT-Client	VMs: 1, Security Policies: 2	-
FT-Server	VMs: 1, Security Policies: 2	+ +

Cancel
Save

2. Go to *Categories > AppType*. Click *Update*. Add FT\_AppType, then save.
3. Go to *Compute & Storage > VMs*. Right-click PC2. Select *Manage Categories*, then set the categories as follows:
  - a. For *Environment*, select *Testing*.
  - b. For *AppType*, select *FT\_AppType*.
  - c. For *AppTier*, select *FT-Client*.
4. Go to *Compute & Storage > VMs*. Right-click PC3. Select *Manage Categories*, then set the categories as follows:
  - a. For *Environment*, select *Testing*.
  - b. For *AppType*, select *FT\_AppType*.
  - c. For *AppTier*, select *FT-Server*.
5. Configure a security policy:
  - a. Go to *Network & Security > Security Policies*. Click *Create Security Policy*, then click *Create*.
  - b. In the *Name* field, enter the desired policy name. In this example, it is FT-Sec\_policy.
  - c. In the *Purpose* field, enter the desired purpose. In this example, it is testing.
  - d. In the *Secure This App* field, select *FT\_AppType*.
  - e. Under *Inbounds*, in the *Add source by: Subnet/IP* field, enter 0.0.0.0/0. Click *Add*.
  - f. Under *Outbounds*, in the *Add source by: Subnet/IP* field, enter 0.0.0.0/0. Click *Add*.
  - g. Under *AppType FT\_AppType*, select *Set rules on App Tiers, instead*. Add *AppTier: FT-Client*, and *FT-Server*.
  - h. Configure the rules:
    - i. For AppTier: FT-Client, create an inbound rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE\_CHAIN. Save.

Create Inbound Rule ✕

---

Subnet/IP 0.0.0.0/0

AppTier FT-Client

**Description**

Enter a description (optional)

**Service Details**

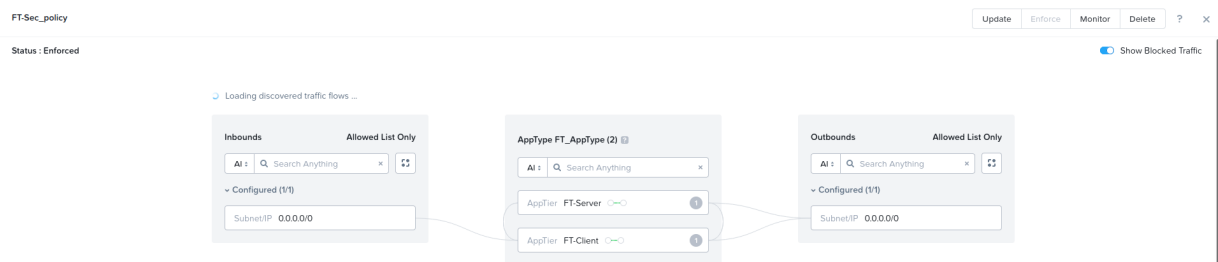
☒ Allow all traffic  
☐ Select a Service

☒ Redirect through a service chain

FORTIGATE\_CHAIN

Cancel Save

- ii. For AppTier: FT-Server, create an inbound rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE\_CHAIN. Save.
  - iii. For AppTier: FT-Client, create an outbound rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE\_CHAIN. Save.
  - iv. For AppTier: FT-Server, create an outbound rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE\_CHAIN. Save.
  - v. For AppTier: FT-Client, create a tier-to-tier rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE\_CHAIN. Save.
  - vi. For AppTier: FT-Server, create a tier-to-tier rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE\_CHAIN. Save.
- i. Under *Select a Policy mode*, select *Enforce*. Click *Save and Enforce*.



### To verify that FortiGate-VM unified threat management works:

1. Verify that pings from PC3 to PC2 go through the FortiGate-VM.
2. Run `diagnose sniffer packet port 3 ' ' 6` to capture ICMP traffic with the vlan30 tag. The following shows example output for this command:

```

Using Original Sniffing Mode
interfaces=[port3]
filters=[]
pcap_lookupnet: port3: no IPv4 address assigned
64.210014 port3 -- 802.1Q vlan#30 P0
0x0000  506b 8d83 af25 506b 8dc2 687d 8100 001e  Pk...%Pk..h)...
0x0010  0800 4500 0054 5145 4000 4001 2c0e c0a8  ..E...TQE@. @.,...
0x0020  1e03 c0a8 1e02 0800 4cd2 0001 0001 84d4  .....L.....
0x0030  2062 0000 0000 4722 0000 0000 0000 1011  .b....G".....
0x0040  1213 1415 1617 1819 1a1b 1c1d 1e1f 2021  .....!.....
0x0050  2223 2425 2627 2829 2a2b 2c2d 2e2f 3031  "##$%&'()*+,-./01
0x0060  3233 3435 3637 234567
64.210125 port3 -- 802.1Q vlan#30 P0
0x0000  506b 8d83 af25 506b 8dc2 687d 8100 001e  Pk...%Pk..h)...
0x0010  0800 4500 0054 5145 4000 4001 2c0e c0a8  ..E...TQE@. @.,...
0x0020  1e03 c0a8 1e02 0800 4cd2 0001 0001 84d4  .....L.....
0x0030  2062 0000 0000 4722 0000 0000 0000 1011  .b....G".....
0x0040  1213 1415 1617 1819 1a1b 1c1d 1e1f 2021  .....!.....
0x0050  2223 2425 2627 2829 2a2b 2c2d 2e2f 3031  "##$%&'()*+,-./01
0x0060  3233 3435 3637 234567
64.210677 port3 -- 802.1Q vlan#30 P0
0x0000  506b 8dc2 687d 506b 8d83 af25 8100 001e  Pk..h)Pk...%....
0x0010  0800 4500 0054 22db 0000 4001 9a78 c0a8  ..E...T"....@...x..
0x0020  1e02 c0a8 1e03 0000 54d2 0001 0001 84d4  .....T.....
0x0030  2062 0000 0000 4722 0000 0000 0000 1011  .b....G".....
0x0040  1213 1415 1617 1819 1a1b 1c1d 1e1f 2021  .....!.....
0x0050  2223 2425 2627 2829 2a2b 2c2d 2e2f 3031  "##$%&'()*+,-./01
0x0060  3233 3435 3637 234567
64.210761 port3 -- 802.1Q vlan#30 P0
0x0000  506b 8dc2 687d 506b 8d83 af25 8100 001e  Pk..h)Pk...%....
0x0010  0800 4500 0054 22db 0000 4001 9a78 c0a8  ..E...T"....@...x..
0x0020  1e02 c0a8 1e03 0000 54d2 0001 0001 84d4  .....T.....
0x0030  2062 0000 0000 4722 0000 0000 0000 1011  .b....G".....
0x0040  1213 1415 1617 1819 1a1b 1c1d 1e1f 2021  .....!.....
0x0050  2223 2425 2627 2829 2a2b 2c2d 2e2f 3031  "##$%&'()*+,-./01
0x0060  3233 3435 3637 234567

```

- Go to **Log & Report > AntiVirus** and verify that unified threat management blocks an eicar.com sample.

The screenshot shows the FortiGate Log & Report interface. The main table displays a log entry for an AntiVirus event. The entry is for a blocked file named 'EICAR\_TEST\_FILE' from 'eicar.com' at IP '192.168.30.3' via 'port3'. The action is 'blocked'.

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
13 seconds ago	HTTP	192.168.30.3	eicar.com	EICAR_TEST_FILE		URL: http://192.168.30.2/eicar.com	blocked

The right-hand pane shows the 'Log Details' for this entry, categorized into several sections:

- General:** Absolute Date/Time: 2022/03/02 13:25:55, Time: 13:25:55, Session ID: 3540, Virtual Domain: root, Agent: curl/7.68.0.
- Source:** IP: 192.168.30.3, Source Port: 46140, Country/Region: Reserved, Source Interface: port2, Source UUID: a837e8a8-61b2-51ec-4cc5-b896bc6a5209, User: (empty).
- Destination:** IP: 192.168.30.2, Port: 80, Country/Region: Reserved, Destination Interface: port3, Destination UUID: a837e8a8-61b2-51ec-4cc5-b896bc6a5209, URL: http://192.168.30.2/eicar.com.
- Application Control:** Protocol: 6, Service: HTTP.
- Data:** File Name: eicar.com.
- Action:** Action: blocked, Threat: 2, Policy ID: VW-Policy (1), Policy UUID: 7d4756a0-88e6-51ec-b2f2-48cc1a1d274e, Policy Type: Firewall.

## Support multiple GCP projects in a single SDN connector - 6.4.7

An option is added to specify multiple projects under a single GCP SDN connector. Previously, only one project was allowed per SDN connector, which limits the total projects to the number of SDN connectors (256). This enhancement also allows dynamic firewall address filters to filter on a project.

In this example, a GCP SDN connector (gcp\_conn) is configured with two projects. The first project, dev-project-001-166400, is configured using the simple format. The second project, dev-project-002, is configured using the advanced format.

### To configure a GCP connector with multiple projects in the GUI:

1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. Select *Google Cloud Platform (GCP)* and enter a name for the connector.
3. Configure the first project:
  - a. For *Projects*, select *Simple*.
  - b. Enter the project name, service account email, and private key.

New External Connector

Public SDN

Google Cloud Platform (GCP)

Connector Settings

Name: gcp\_conn

Status: ☒ Enabled ☐ Disabled

Update interval: ☒ Use Default ☐ Specify

GCP Connector

Projects: ☒ Simple ☐ Advanced

Name: dev-project-001-166400

Service account email: compute@developer.gserviceaccount.com 50/127

Private key: -----BEGIN PRIVATE KEY-----  
 MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC...  
 -----END PRIVATE KEY-----

Public SDN Connector Setup Guides

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Oracle Cloud Infrastructure

Private SDN Connector Setup Guides

- Cisco Application Centric Infrastructure
- Nuage Virtualized Services Platform
- OpenStack Connector
- VMware NSX

Documentation

- Online Help
- Video Tutorials

OK Cancel

## 4. Configure the second project:

- a. For *Projects*, select *Advanced* (the projects are now displayed in a table) and click *Create New*.

The *Add GCP Project* pane opens.

- b. Enter a name.
- c. Optionally, click the + to enter zones. If no zones are selected, the SDN connector will include all zones. The *us-central1-a* zone is used in this example.

- d. Click *OK*.

5. Click *OK* to save the SDN connector.

## 6. Create a dynamic firewall address for the first project:

- a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
- b. Enter the following:

<b>Name</b>	project1_addresses
<b>Type</b>	Dynamic



<b>Sub Type</b>	Fabric Connector Address
<b>SDN Connector</b>	gcp_conn
<b>Filter</b>	Add a filter for the project, <i>Project=dev-project-001-166400</i> . In this example, there are several instances for the first project, so add a filter for the ID, <i>Id=6266132824476267466</i> . Change the logic operator to <i>and</i> .

c. Click **OK**.

7. Create a dynamic firewall address for the second project:

a. Click *Create New > Address*.

b. Enter the following:

<b>Name</b>	project2_addresses
<b>Type</b>	Dynamic
<b>Sub Type</b>	Fabric Connector Address
<b>SDN Connector</b>	gcp_conn
<b>Filter</b>	Add a filter for the project, <i>Project=dev-project-002</i> .

c. Click **OK**.

The addresses have been created. Wait for a few minutes before the settings take effect.

8. Verify that the address resolve to the correct addresses. Hover over the address in the table to view the list of populated IP addresses.

### To configure a GCP connector with multiple projects in the CLI:

1. Configure the SDN connector:

```
config system sdn-connector
  edit "gcp_conn"
    set status enable
    set type gcp
    config gcp-project-list
      edit "dev-project-001-166400"
```

```

        next
        edit "dev-project-002"
            set gcp-zone-list "us-central1-a"
        next
    end
    set service-account "xxxxxxxxxxxx-compute@developer.gserviceaccount.com"
    set private-key *****
    set update-interval 30
next
end

```

## 2. Create a dynamic firewall address for project one:

```

config firewall address
    edit "project1_addresses"
        set type dynamic
        set sdn "gcp_conn"
        set filter "Project=dev-project-001-166400 & Id=6266132824476267466"
    next
end

```

The dynamic firewall address IP is resolved by the SDN connector:

```

config firewall address
    edit "project1_addresses"
        show
        config firewall address
            edit "project1_addresses"
                set uuid 38efbd88-fb08-51eb-8e6d-9b78a2a9bf49
                set type dynamic
                set sdn "gcp_conn"
                set filter "Project=dev-project-001-166400 & Id=6266132824476267466"
                config list
                    edit "172.16.16.3"
                    next
                    edit "172.16.24.3"
                    next
                    edit "172.16.8.4"
                    next
                end
            next
        end
    next
end

```

## 3. Create a dynamic firewall address for project two:

```

config firewall address
    edit "project2_addresses"
        set type dynamic
        set sdn "gcp_conn"
        set filter "Project=dev-project-002"
        set sdn-addr-type all
    next
end

```

The dynamic firewall address IP is resolved by the SDN connector:

```

config firewall address
  edit "project2_addresses"
    show
    config firewall address
      edit "project2_addresses"
        set uuid 5ca9b2ba-fb08-51eb-57c0-12701b3d33c1
        set type dynamic
        set sdn "gcp_conn"
        set filter "Project=dev-project-002"
        set sdn-addr-type all
        config list
          edit "10.128.0.2"
          next
          edit "34.66.35.241"
          next
        end
      next
    end
  next
end

```

## Ciphers added to fips-ciphers mode on FortiGate-VM - 6.4.7

FortiGate-VM `fips-ciphers` mode has added new ciphers so that cloud instances running this mode can establish IPsec VPN tunnels with hardware models running FIPS-CC mode. This feature is available for FortiGate-VMs deployed on AWS, Azure, Google Cloud, and OCI.

`fips-cipher` mode supports the following ciphers for IPsec VPN:

### Phase-1:

aes128-sha256	aes128-sha256
aes128-sha384	aes128-sha384
aes128-sha512	aes128-sha512
aes128gcm-prfsha256	aes128gcm-prfsha256
aes128gcm-prfsha384	aes128gcm-prfsha384
aes128gcm-prfsha512	aes128gcm-prfsha512
aes256-sha256	aes256-sha256
aes256-sha384	aes256-sha384
aes256-sha512	aes256-sha512
aes256gcm-prfsha256	aes256gcm-prfsha256
aes256gcm-prfsha384	aes256gcm-prfsha384
aes256gcm-prfsha512	aes256gcm-prfsha512

### Phase-2:

aes128-sha256	aes128-sha256
aes128-sha384	aes128-sha384
aes128-sha512	aes128-sha512
aes128gcm	aes128gcm
aes256-sha256	aes256-sha256
aes256-sha384	aes256-sha384
aes256-sha512	aes256-sha512
aes256gcm	aes256gcm

# FortiCarrier

This section includes information about FortiCarrier related new features:

- [GTP on page 550](#)

## GTP

This section includes information about GTP related new features:

- [IPv6 support for GTP 6.4.2 on page 550](#)
- [Add fields to correlate between traffic, GTP, and UTM logs 6.4.2 on page 552](#)
- [Multiple identities from the ULI field in GTP logs 6.4.2 on page 554](#)
- [NPU support for GTP-U encapsulated in IPv6 6.4.3 on page 554](#)

## IPv6 support for GTP - 6.4.2

FortiOS Carrier supports IPv6 only and IPv4/IPv6 dual stack for GTPv1 and GTPv2.

### IPv6 in GTP configuration

```
config firewall gtp
  edit "gtpp"
    set handover-group6 <sgsnv6_grp_addr>
    set authorized-sgsns6 <sgsnv6_grp_addr>
    set invalid-sgsns6-to-log <sgsnv6_grp_addr>
    set authorized-ggsns6 <ggsnv6_grp_addr>
    config ie-remove-policy
      edit 1
        set sgsn-addr6 <sgsnv6>
      next
    end
    config ip-policy
      edit 1
        set srcaddr6 "all"
        set dstaddr6 "all"
      next
    end
  next
end
```

### Diagnose commands

#### Mobile user IPv6 address

```
diagnose firewall gtp tunnel filter ms-addr6 <from_ipv6_address> <to_ipv6_address>
```

### IPv6 address of the control plane F-TEID

This is only applicable to GTPv1 and GTPv2 tunnels.

```
diagnose firewall gtp tunnel filter f-teid-c addr6 <from_ipv6_address> <to_ipv6_address>
```

### IPv6 address of the data plane F-TEID

This is only applicable to GTPv1 and GTPv2 tunnels.

```
diagnose firewall gtp tunnel filter f-teid-u addr6 <from_ipv6_address> <to_ipv6_address>
```

### Clear the mobile user IPv6 address filter

```
diagnose firewall gtp tunnel filter clear ms-addr6
```

### Clear the IPv6 address of the control or data plane F-TEID filter

```
diagnose firewall gtp tunnel filter clear {f-teid-c | f-teid-u} addr6
```

### Inverse mobile user IPv6 address filter

```
diagnose firewall gtp tunnel filter negate ms-addr6
```

### IPv6 handover group

```
# diagnose firewall gtp handover-grp6 show gtp
print gtp IPv6 handover group
[2001:10:1:100::-2001:10:1:100:ffff:ffff:ffff:ffff], [2002:10:1:100::-
2002:10:1:100:ffff:ffff:ffff:ffff],
```

### Authorized IPv6 SGSNs

```
# diagnose firewall gtp auth-sgsns6 show gtp
print gtp IPv6 authorized SGSNs
[2001:10:1:100::-2001:10:1:100:ffff:ffff:ffff:ffff], [2002:10:1:100::-
2002:10:1:100:ffff:ffff:ffff:ffff],
```

### Invalid IPv6 SGSNs to be logged

```
# diagnose firewall gtp invalid-sgsns6-to-log show gtp
print gtp IPv6 invalid SGSNs to be logged
[2001:10:1:100::-2001:10:1:100:ffff:ffff:ffff:ffff], [2002:10:1:100::-
2002:10:1:100:ffff:ffff:ffff:ffff],
```

### Authorized IPv6 GGSNs

```
# diagnose firewall gtp auth-ggsns6 show gtp
print gtp IPv6 authorized GGSNs
[2001:172:16:200::-2001:172:16:200:ffff:ffff:ffff:ffff], [2002:172:16:200::-
2002:172:16:200:ffff:ffff:ffff:ffff],
```

## IPv6 GTP log example

```
date=2020-06-26 time=15:01:27 logid="1400041224" type="gtp" subtype="gtp-all"
level="information" vd="vdom1" eventtime=1593208887251968776 tz="-0700" profile="gtp"
status="prohibited" version=2 msg-type=32 from6=2001:172:16:200::6 to6=2001:172:16:200::34
deny_cause="sgsn-not-authorized" ietype=75 dtlexp="none" srcport=34612 dstport=2123 seqnum=1
tunnel-idx=0 imsi="021310123200000" msisdn="12345678900001" apn="apn2.com" selection="apns-
vrf" imei-sv="unknown" rat-type="eutran" end-usr-address=11.0.1.50 headerteid=0
snetwork="222.333" cpaddr6=2001:10:1:100::33 cpteid=886008 uli="011000:222.333.1" ulimcc=222
ulimnc=333
```

```
date=2020-06-26 time=15:04:23 logid="1400041223" type="gtp" subtype="gtp-all"
level="information" vd="vdom1" eventtime=1593209063197162647 tz="-0700" profile="gtp"
status="forwarded" version=2 msg-type=32 from6=2001:172:16:200::6 to6=2001:172:16:200::34
srcport=65372 dstport=2123 seqnum=1 tunnel-idx=4 imsi="021310123200000"
msisdn="12345678900001" apn="apn2.com" selection="apns-vrf" imei-sv="unknown" rat-
type="eutran" end-usr-address=11.0.1.50 headerteid=0 snetwork="222.333"
cpaddr6=2001:10:1:100::33 cpteid=886008 uli="011000:222.333.1" ulimcc=222 ulimnc=333
```

```
date=2020-06-26 time=15:08:03 logid="1400041228" type="gtp" subtype="gtp-all"
level="information" vd="vdom1" eventtime=1593209283529236672 tz="-0700" profile="gtp"
status="traffic-count" version=2 cpdladdr6=2001:10:1:100::33 cpdlteid=886008 cpdlisrteid=0
cpulteid=0 tunnel-idx=4 duration=220 c-pkts=1 c-bytes=262 u-pkts=0 u-bytes=0
imsi="021310123200000" msisdn="12345678900001" apn="apn2.com" selection="apns-vrf" imei-
sv="unknown" rat-type="eutran" end-usr-address=11.0.1.50 snetwork="222.333"
uli="011000:222.333.1" ulimcc=222 ulimnc=333
```

## Add fields to correlate between traffic, GTP, and UTM logs - 6.4.2

The tunnel ID is added to traffic and GTP logs for GTP-related traffic in order to correlate the sessions. The session ID can be used to correlate between traffic logs and UTM logs. This feature requires IPS Engine version 6.026 and later.

The following diagnose commands have been added:

```
diagnose ips share list gtp-u_db
diagnose ips gtp {list | clear | stats | stats-clear} [vdom]
```

### Sample CLI output:

```
(global) # diagnose ips share list gtp-u_db
GTP-U: vf:1 uplink:1 downlink:1 expiry:275
GTP-C: uplink:1 downlink:1 pid:507

(global) # diagnose ips gtp list 1

path:1 vd:1 172.16.200.61:2123 10.1.100.60:2123 echo:0 expiry:358
  tunnel 1: uteid:1 dteid:1 expiry:58
    bearer 1: uteid:1 dteid:1
```

### Sample traffic log:

```
(vdom1) # execute log filter category 0
(vdom1) # execute log display
3 logs found.
3 logs returned.
```

```
1: date=2020-07-03 time=17:52:26 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1593823946988134933 tz="-0700" srcip=10.1.100.60
srcport=2152 srcintf="port2" srcintfrole="undefined" dstip=172.16.200.61 dstport=2152
dstintf="port1" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
sessionid=450 proto=17 action="accept" policyid=1 policytype="policy" poluuid="74b34458-
bcbf-51ea-f0ec-1a54736a54c1" policyname="11" service="GTP" trandisp="noop" duration=334
sentbyte=4435 rcvdbyte=5351 sentpkt=31 rcvdpkt=23 appcat="unscanned" sentdelta=184
rcvddelta=820 utmref=0-42
```

```
2: date=2020-07-03 time=17:51:27 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1593823887326990647 tz="-0700" srcip=192.168.0.2
srcport=57913 srcintf="port2" srcintfrole="undefined" dstip=192.168.0.1 dstport=80
dstintf="port1" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
sessionid=5 proto=6 action="accept" policyid=1 policytype="policy" policyname="11"
tunnelid=1 service="HTTP" trandisp="snat" transip=0.0.0.0 transport=0 duration=179
sentbyte=147 rcvdbyte=318 sentpkt=0 rcvdpkt=0 appcat="unscanned" utmaction="block"
countips=1 utmref=0-28
```

```
3: date=2020-07-03 time=17:50:30 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1593823830269870321 tz="-0700" srcip=192.168.0.2
srcport=37029 srcintf="port2" srcintfrole="undefined" dstip=192.168.0.1 dstport=80
dstintf="port1" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved"
sessionid=3 proto=6 action="accept" policyid=1 policytype="policy" policyname="11"
tunnelid=1 service="HTTP" trandisp="snat" transip=0.0.0.0 transport=0 duration=213
sentbyte=138 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appid=15893 app="HTTP.BROWSER"
appcat="Web.Client" apprisk="medium" utmaction="block" countapp=1 utmref=0-14
```

### Sample GTP log:

```
19: date=2020-07-03 time=17:48:27 logid="1400041229" type="gtp" subtype="gtp-all"
level="information" vd="vdom1" eventtime=1593823707831428535 tz="-0700" profile="gtp"
status="forwarded" version=1 msg-type=255 from=172.16.200.61 to=10.1.100.60 srcport=2152
dstport=2152 headerteid=1 tunnel-idx=1 imsi="310150123456789" msisdn="6044301297"
apn="unknown"
```

```
47: date=2020-07-03 time=17:46:56 logid="1400041229" type="gtp" subtype="gtp-all"
level="information" vd="vdom1" eventtime=1593823616760095386 tz="-0700" profile="gtp"
status="forwarded" version=1 msg-type=255 from=10.1.100.60 to=172.16.200.61 srcport=2152
dstport=2152 headerteid=1 tunnel-idx=1 imsi="310150123456789" msisdn="6044301297"
apn="unknown"
```

### Sample matched UTM log:

```
(vdom1)# execute log detail 4 0-28
1 logs found.
1 logs returned.
```

```
1: date=2020-07-03 time=17:48:27 logid="0419016384" type="utm" subtype="ips"
eventtype="signature" level="alert" vd="vdom1" eventtime=1593823707631357842 tz="-0700"
severity="info" srcip=192.168.0.2 srccountry="Reserved" dstip=192.168.0.1 sessionid=5
action="dropped" proto=6 service="HTTP" policyid=1 attack="Eicar.Virus.Test.File"
srcport=57913 dstport=80 hostname="192.168.0.1" url="/eicar.com" direction="incoming"
attackid=29844 profile="gtp-ips-profile" ref="http://www.fortinet.com/ids/VID29844"
incidentserialno=155189252 msg="file_transfer: Eicar.Virus.Test.File,"
```

```
(vdom1) # execute log detail 10 0-14
1 logs found.
1 logs returned.
```

```
1: date=2020-07-03 time=17:46:56 logid="1059028705" type="utm" subtype="app-ctrl"
eventtype="signature" level="warning" vd="vdom1" eventtime=1593823616148659619 tz="-0700"
appid=15893 srcip=192.168.0.2 dstip=192.168.0.1 srcport=37029 dstport=80 proto=6
service="HTTP" direction="outgoing" policyid=1 sessionid=3 applist="gtp-appctrl-profile"
action="block" appcat="Web.Client" app="HTTP.BROWSER" hostname="192.168.0.1"
incidentserialno=155189251 url="/" msg="Web.Client: HTTP.BROWSER," apprisk="medium"
```

## Multiple identities from the ULI field in GTP logs - 6.4.2

In GTP, User Location Information (ULI) can contain multiple identities of different types.

All identity information is included in GTP logs in the following format:

```
uli="<type1>:<value1>|<type2>:<value2>|...|<typen>:<valuen>"
```

### GTP log with one ULI field:

```
date=2020-07-16 time=14:33:21 logid="1400041223" type="gtp" subtype="gtp-all"
level="information" vd="root" eventtime=1594449111699047715 tz="-0700"
profile="default" status="forwarded" version=2 msg-type=32 from=9.8.3.19 to=9.8.8.19
srcport=2123 dstport=2123 seqnum=6408905 tunnel-idx=9924610 imsi="240011334567000"
msisdn="140541334560000" apn="internet" selection="apns-vrf" imei-sv="35911300.0.0"
end-usr-address=192.168.4.1 headerteid=0 snetwork="310.13" cpaddr=9.8.3.19 cpteid=1
uli="LAI:813.1.2112" ulimcc=813 ulimnc=1
```

### GTP log with two ULI fields:

```
date=2020-07-16 time=14:41:18 logid="1400041223" type="gtp" subtype="gtp-all"
level="information" vd="root" eventtime=1594449138757040276 tz="-0700"
profile="default" status="forwarded" version=2 msg-type=32 from=9.8.3.19 to=9.8.8.19
srcport=2123 dstport=2123 seqnum=6408906 tunnel-idx=9924611 imsi="240011334567001"
msisdn="140541334560001" apn="internet" selection="apns-vrf" imei-sv="35911300.1.0"
rat-type="eutran" end-usr-address=192.168.4.2 headerteid=0 snetwork="310.13"
cpaddr=9.8.3.19 cpteid=2 uli="RAI:180.203.1124.61|LAI:311.289.3792" ulimcc=180
ulimnc=203
```

### GTP log with six ULI fields:

```
date=2020-07-16 time=15:35:59 logid="1400041223" type="gtp" subtype="gtp-all"
level="information" vd="root" eventtime=1594449119716113782 tz="-0700"
profile="default" status="forwarded" version=2 msg-type=32 from=9.8.3.19 to=9.8.8.19
srcport=2123 dstport=2123 seqnum=6408905 tunnel-idx=9924610 imsi="240011334567000"
msisdn="140541334560000" apn="internet" selection="apns-vrf" imei-sv="35911300.0.0"
end-usr-address=192.168.4.1 headerteid=0 snetwork="310.13" cpaddr=9.8.3.19 cpteid=1
uli="CGI:813.1.2112.4613|SAI:1.252.4253.E331|RAI:180.203.1124.61|TAI:205.421.253E|ECGI
:338.311.211246|LAI:310.120.5242" ulimcc=813 ulimnc=1
```

## NPU support for GTP-U encapsulated in IPv6 - 6.4.3

The `gtp-enhanced-mode` parameter under `config system npu` can enable offloading GTP-U traffic.



**To enable GTP enhancement mode:**

```
config system npu
    set gtp-enhanced-mode enable
end
```

After the IPv6 GTP tunnel has been established and there is GTP-U traffic, verify the IPv6 session list to confirm those sessions were offloaded to NPU (GTPU\_offload). The NPU packet count can also be verified.

**To verify the IPv6 session list:**

```
# diagnose sys session6 list

session6 info: proto=17 proto_state=01 duration=3 expire=179 timeout=0 flags=00000000
sockport=0 socktype=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=gtp-c vlan_cos=0/0
state=may_dirty npu npd
statistic(bytes/packets/allow_err): org=339/2/0 reply=232/2/0 tuples=2
tx speed(Bps/kbps): 104/0 rx speed(Bps/kbps): 71/0
origin->sink: org pre->post, reply pre->post dev=34->33/33->34
hook=pre dir=org act=noop 2000:119:10:10::1:2123 ->2000:120:41:30::1:2123 (:::0)
hook=post dir=reply act=noop 2000:120:41:30::1:2123 ->2000:119:10:10::1:2123 (:::0)
gtp=gtp
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000087cc tos=ff/ff ips_view=0 app_list=0 app=0 url_cat=0
ngfwid=n/a
npu_state=0x100000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason: offload-denied helper

session6 info: proto=17 proto_state=01 duration=0 expire=179 timeout=0 flags=00000000
sockport=0 socktype=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=gtp-u vlan_cos=0/0
state=may_dirty npu
statistic(bytes/packets/allow_err): org=268/2/0 reply=272/2/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=34->33/33->34
hook=pre dir=org act=noop 2000:119:10:10::1:2152 ->2000:120:41:30::1:2152 (:::0)
hook=post dir=reply act=noop 2000:120:41:30::1:2152 ->2000:119:10:10::1:2152 (:::0)
gtp=gtp
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000087cf tos=ff/ff ips_view=0 app_list=0 app=0 url_cat=0
ngfwid=n/a
npu_state=0x000e00 GTPU_offload
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=107/107, ipid=494/488,
vlan=0x0000/0x0000
vlifid=494/488, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=25/25
```

**To verify the NPU packet count:**

```
# diagnose npu np6 hbq-stats all
  cpu_ 0:0
  ...
  cpu_52:73
  ...
Total   :73
```

# FortiASIC

This section includes information about FortiASIC related new features:

- [Hardware acceleration on page 557](#)

## Hardware acceleration

This section includes information about hardware acceleration related new features:

- [Use CP9/SoC3 entropy source on page 557](#)
- [Identify the XAUI link used for a specific traffic stream on page 557](#)

### Use CP9/SoC3 entropy source

FortiGate models that use FortiASIC CP9 and SoC3 chips periodically reseed a PRNG (Pseudo-Random Number Generator) in normal (non-CC/FIPS) mode.

### Identify the XAUI link used for a specific traffic stream

The `diagnose npu np6 xau-hash` command takes a 6-tuple input of the traffic stream to identify the NP6 XAUI link that the traffic passes through.

This command is only available on the 38xxD, 39xxD, 34xxE, 36xxE, and 5001E series devices.

#### Syntax

```
diagnose npu np6 xau-hash <interface> <proto> <src_ip> <dst_ip> <src_port> <dst_port>
```

Variable	Description
<interface>	The network interface that the packets are coming from.
<proto>	The proto number, 6 for TCP or 17 for UDP.
<src_ip>	The source IP address.
<dst_ip>	The destination IP address.
<src_port>	The source port.
<dst_port>	The destination port.

#### Examples

```
# diagnose npu np6 xau-hash port1 6 1.1.1.1 2.2.2.1 4567 80
NP6_ID: 0, XAUI_LINK: 2
```

```
# diagnose npu np6 xau-hash port1 6 1.1.1.1 2.2.2.1 4567 200
NP6_ID: 6, XAUI_LINK: 2

# diagnose npu np6 xau-hash port1 6 1.1.1.1 2.2.2.1 4567 20
NP6_ID: 1, XAUI_LINK: 2

# diagnose npu np6 xau-hash port1 6 1.1.1.1 2.2.2.1 4567 23
NP6_ID: 1, XAUI_LINK: 1
```

The `NP6_ID` is the NP index of the model that is being used. It can be found with the `diagnose npu np6 port-list` command.



**FORTINET®**



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.